Enhancements to 802.1D and PVST+

Cabrillo College

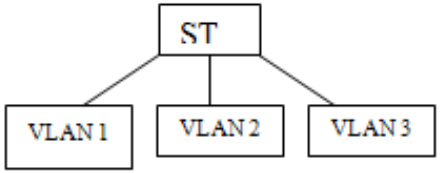
CIS 187 Multilayer Switched Networks

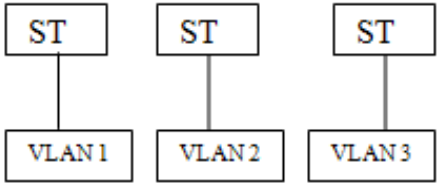
CCNP 3 version 4

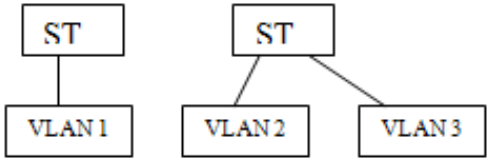
Rick Graziani

Fall 2006

Evolution of STP

Cisco's Implementation	Spanning Tree Protocol Process	IEEE Standard
Spanning Tree Protocol (STP): • 802.1D • Common Spanning Tree (CST) • Mono Spanning Tree (MST)	ST = Spanning Tree 	
Cisco Enhancements (First evolution): • Portfast • Uplinkfast • Backbonefast		RSTP: • 802.1w • Edge Fast (Cisco Port Fast) • Uplink Fast RSTP (Cisco Uplink Fast) • Backbone Fast Engine (Cisco Backbone Fast)

Cisco Enhancements (Second Evolution):
• PVST: ISL
• PVST+: ISL & 802.1Q
• Includes previous enhancements
• Additional enhancements:
  ○ BPDU Guard
  ○ Root Guard
		

Cisco MISTP: • Uses PVST+ • Includes previous enhancements • Catalyst 4000/6000		MST (Multiple Spanning Tree): • 802.1s • Uses RSTP

IEEE Documents

- IEEE 802.1D - Media Access Control (MAC) bridges
- IEEE 802.1Q - Virtual Bridged Local Area Networks
- IEEE 802.1w - Rapid Reconfiguration (Supp. To 802.1D)
- IEEE 802.1s - Multiple Spanning Tree (Supp. To 802.1Q)
- IEEE 802.1t - Local and Metropolitan Area Network: Common Specifications

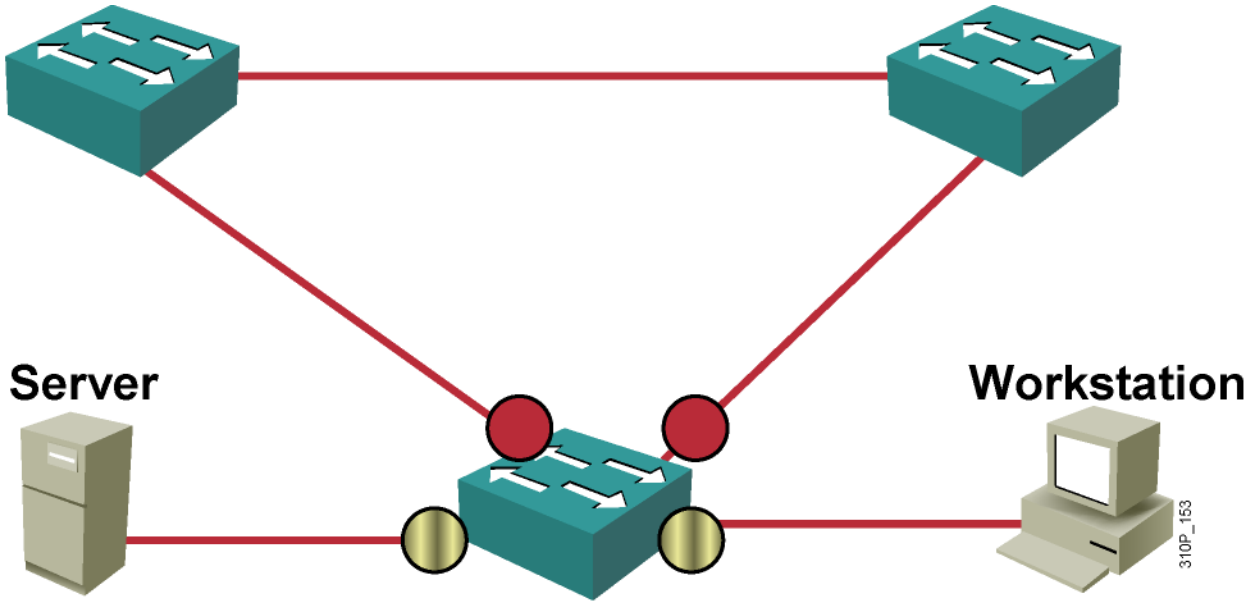
Enhancements to STP

- PortFast
- Per VLAN Spanning Tree (PVST+)
- Rapid Spanning Tree Protocol (RSTP)
- Multiple Spanning Tree Protocol (MSTP)
  - MSTP is also known as Multiple Instance Spanning Tree Protocol (MISTP) on Cisco Catalyst 6500 switches and above
- Per VLAN Rapid Spanning Tree (PVRST)

Portfast

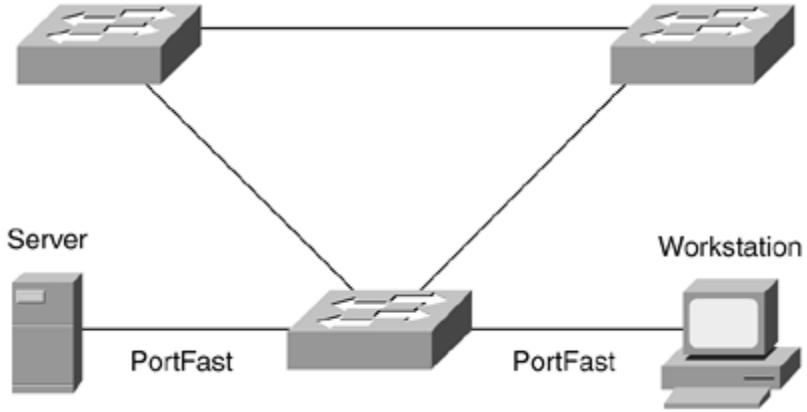
PortFast

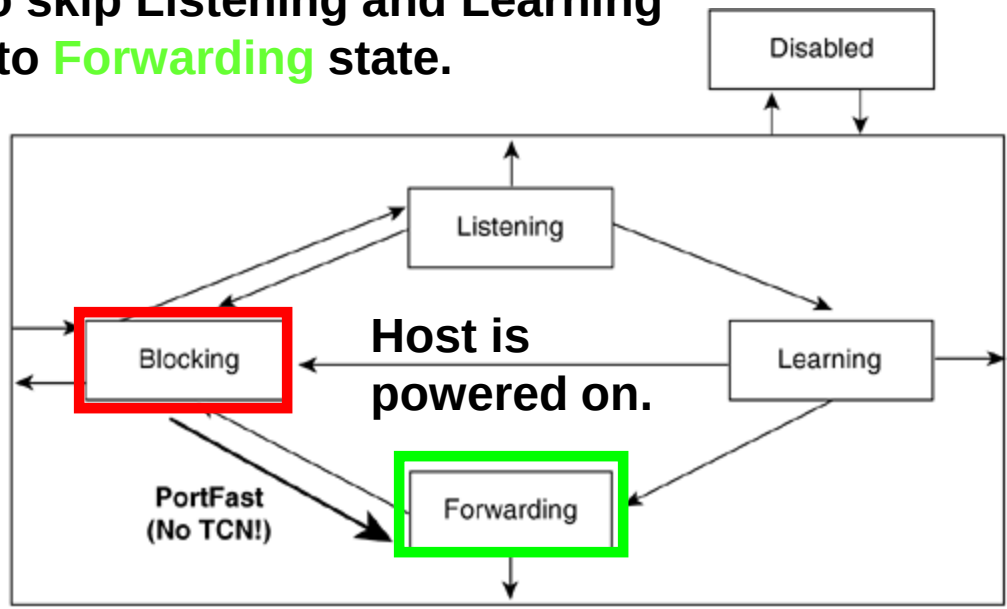
- By using PortFast, devices can be granted instant access to the Layer 2 network without going through the spanning tree listening and learning stages.



PortFast

Portfast causes port to skip Listening and Learning and immediately go into Forwarding state.





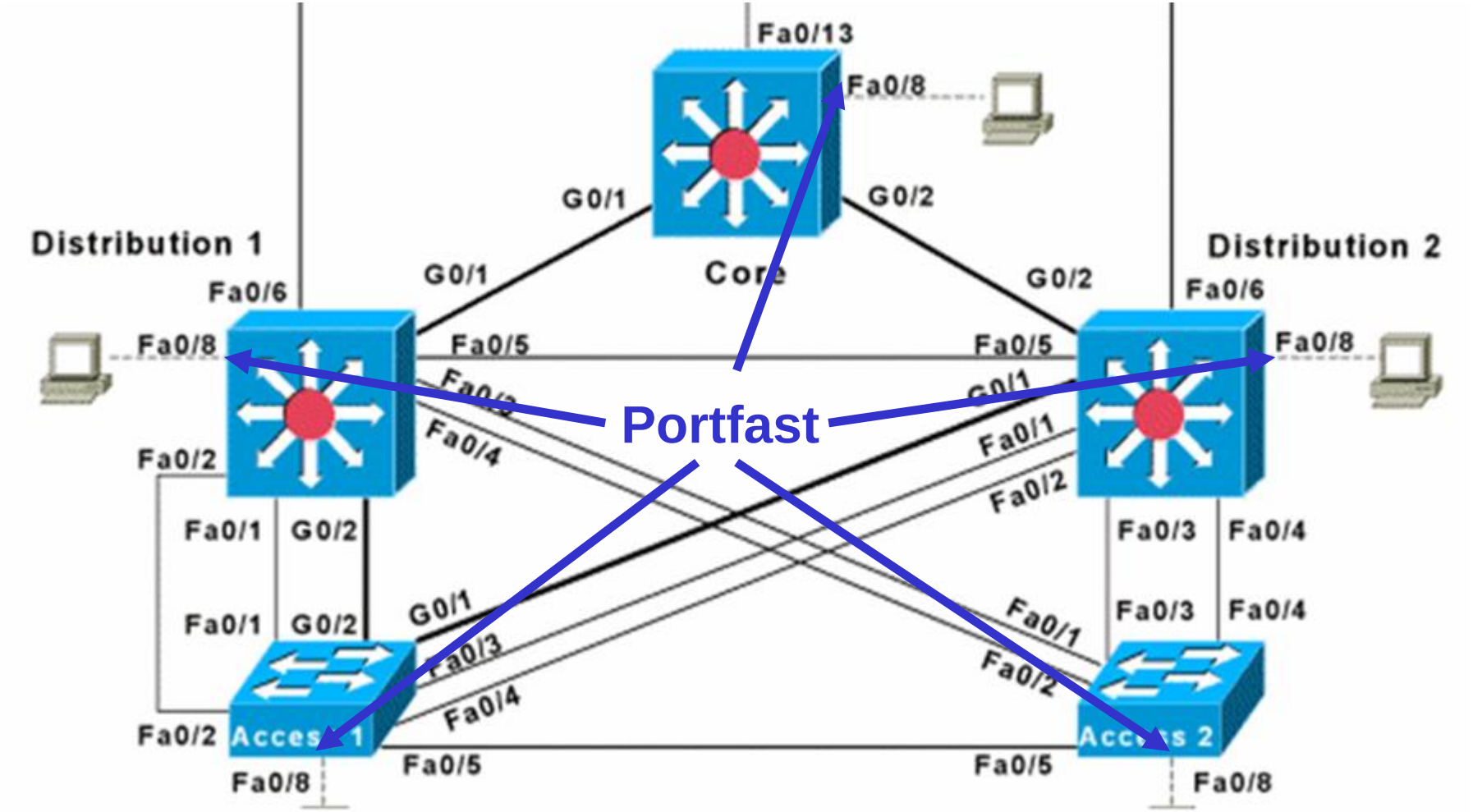
- Enable PortFast on Layer 2 access ports connected to a single workstation or server to allow those devices to connect to the network immediately, rather than waiting for spanning tree to converge.
- The purpose of PortFast is to minimize the time that access ports wait for STP to converge.
- The advantage of enabling PortFast is to prevent **DHCP** timeouts.

Configuring Portfast

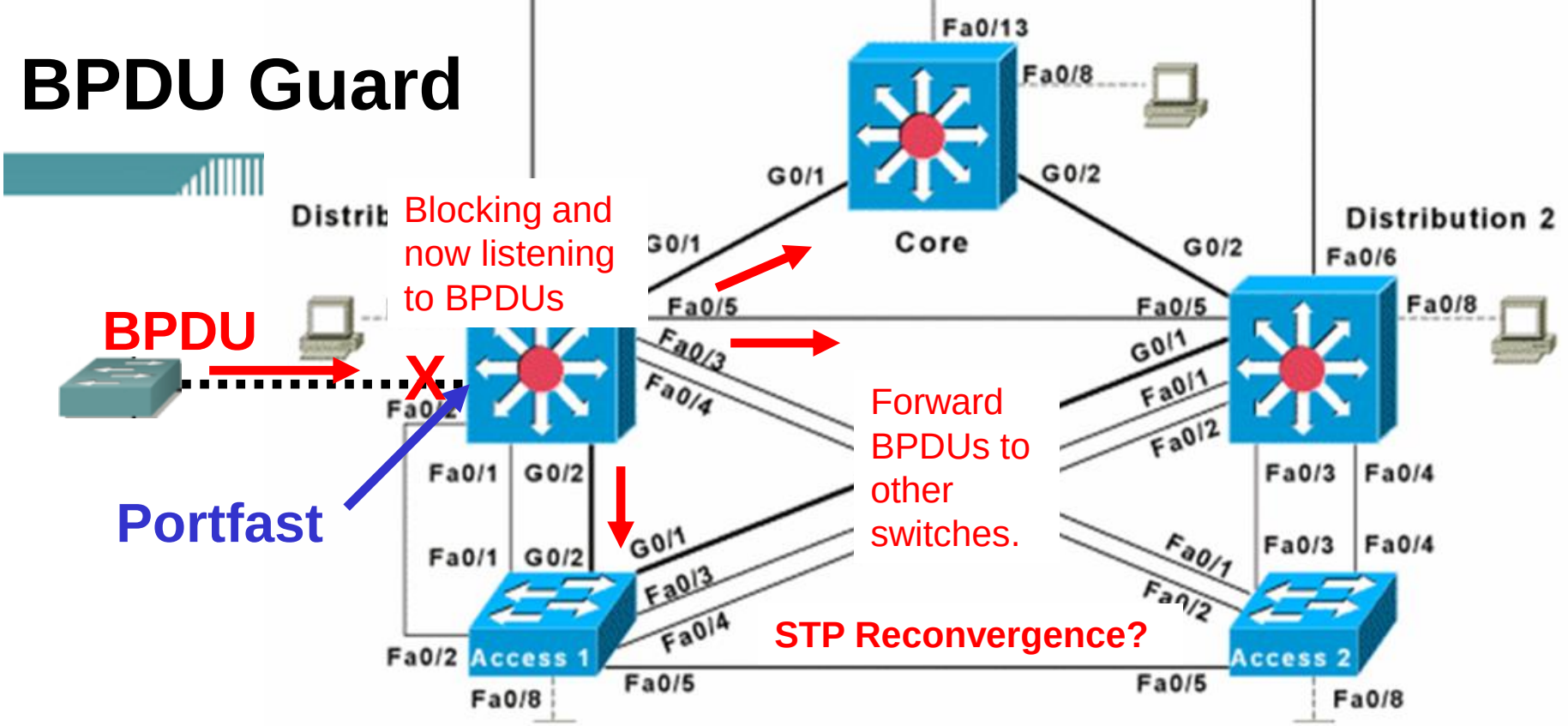

```
Access2(config)#interface range fa 0/6 - 12
Access2(config-if-range)#switchport mode access
Access2(config-if-range)#spanning-tree portfast
    OR
Access2(config)#spanning-tree portfast default
```

- **Warning:** PortFast should only be enabled on ports that are connected to a single host.
- If hubs, concentrators, switches, and bridges. are connected to the interface when PortFast is enabled, temporary bridging loops can occur.
- Use with caution.
- Use the following command to enable PortFast globally in global configuration mode:

- **Portfast** is configured on all access mode ports.



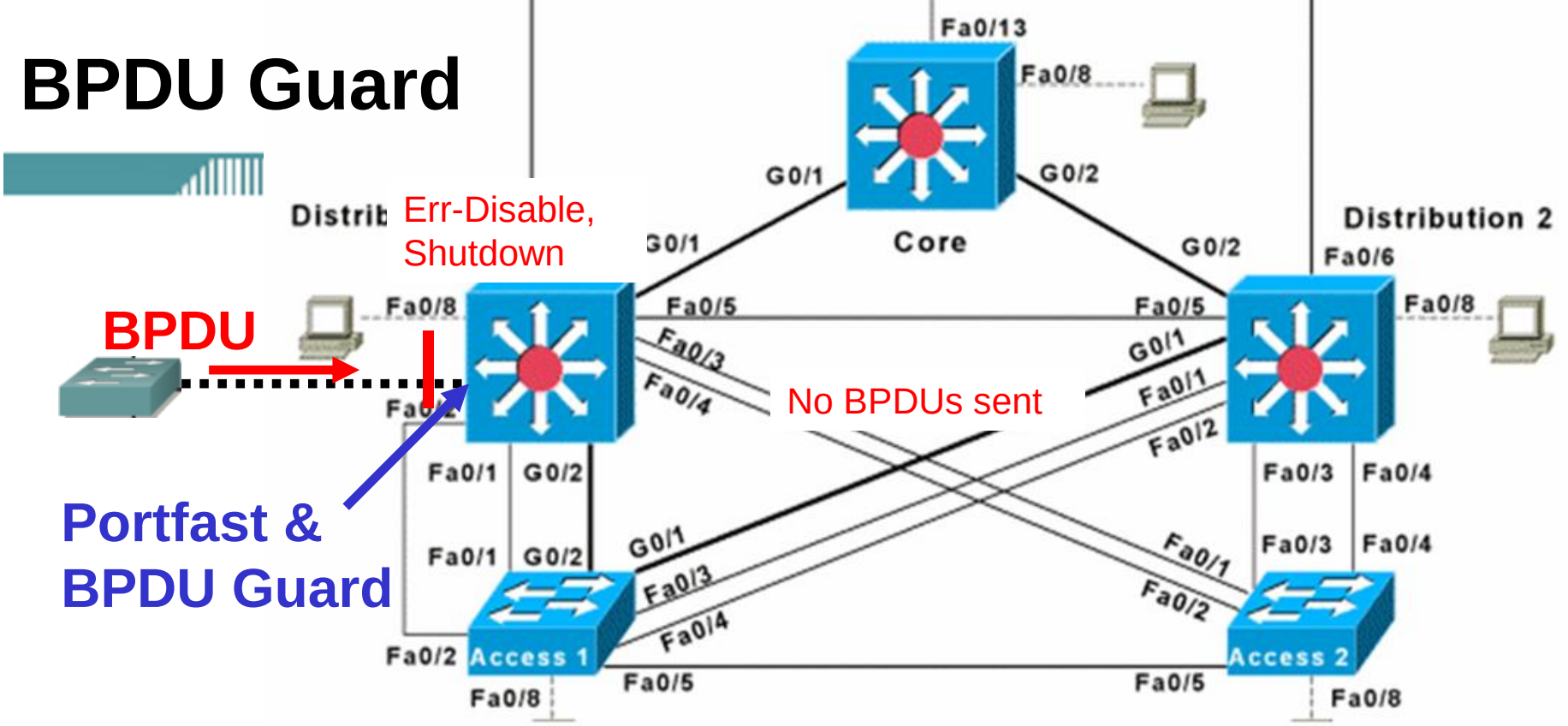
BPDU Guard



- Enabling PortFast can create a security risk in a switched network.
- A port configured with PortFast will go into **blocking** state if it receives a Bridge Protocol Data Unit (**BPDU**).
- An unauthorized device can send BPDUs into the PortFast interface and set a port to blocking.
- When the port is in blocking state it will accept all BPDUs.
- This could lead to false STP information that enters the switched network and causes unexpected STP behavior.

BPDU Guard

BPDU Guard

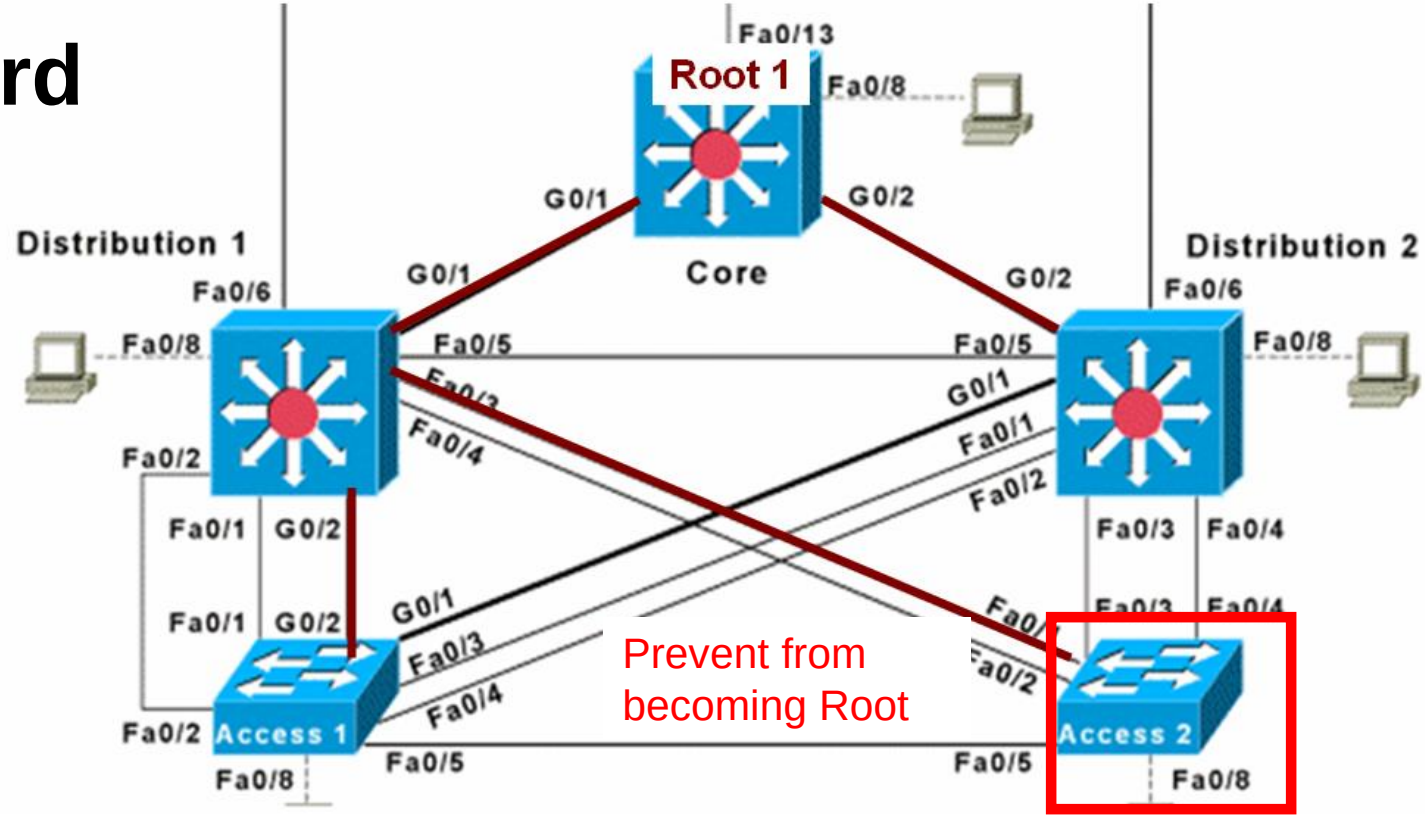



```
Access2(config)#interface range fa 0/6 - 12
Access2(config-if-range)#spanning-tree bpduguard enable
```

- When the BPDU guard feature is enabled on the switch, STP shuts down PortFast enabled interfaces that receive BPDUs instead of putting them into a blocking state.
- PortFast-enabled interfaces do not receive BPDUs in a valid configuration.
- The BPDU guard feature blocks BPDUs by placing the interface in the ErrDisable state.
- BPDU guard will also keep switches added outside the wiring closet by users from impacting and possibly violating Spanning Tree Protocol.

Root Guard

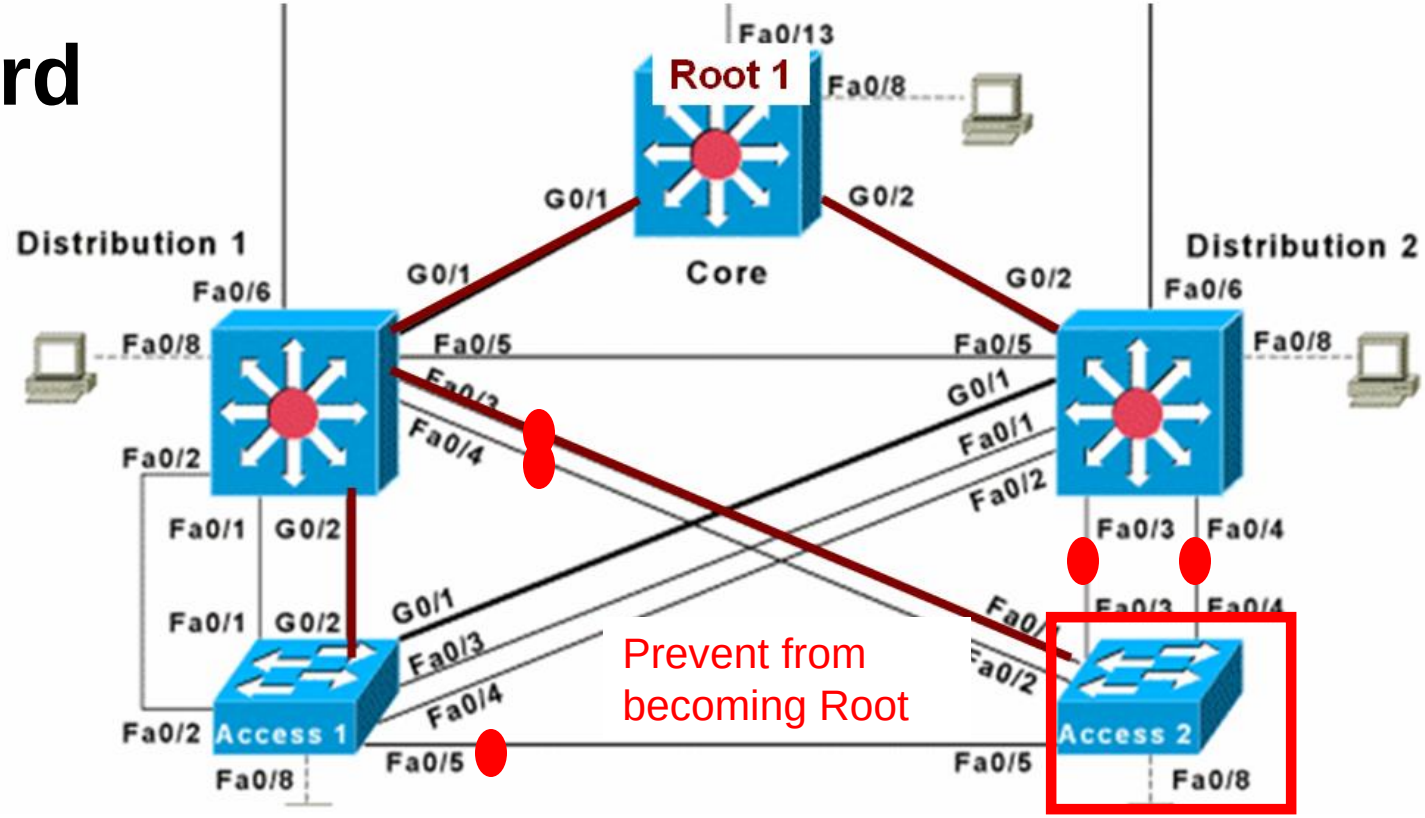
Root Guard



- Root Guard is used if the network administrator wants to prevent a switch (usually access switch) from becoming the root bridge or from being in the path to the root bridge.
- Root guard will be used to prevent switches from becoming the root bridge.
- Configured on switches that connect to this switch.

Root Guard

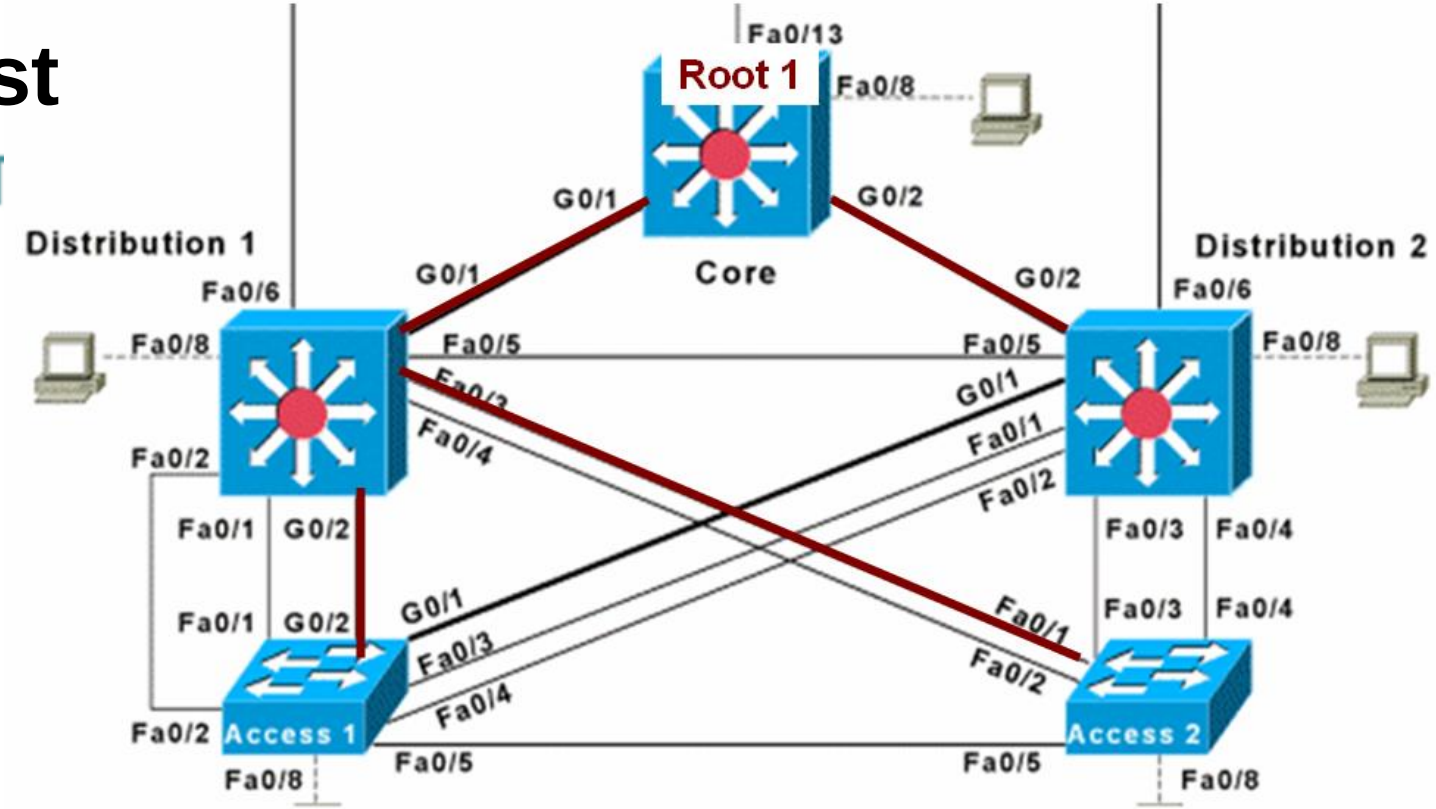
- UplinkFast must be disabled because it cannot be used with root guard.




```
Distribution1(config)#interface range fa 0/3 - 4
Distribution(config-if-range)#spanning-tree guard root

Distribution2(config)#interface range fa 0/3 - 4
Distribution(config-if-range)#spanning-tree guard root

Access1(config)#interface fa 0/5
Access1(config-if)#spanning-tree guard root

Access2(config)#no spanning-tree uplinkfast
```

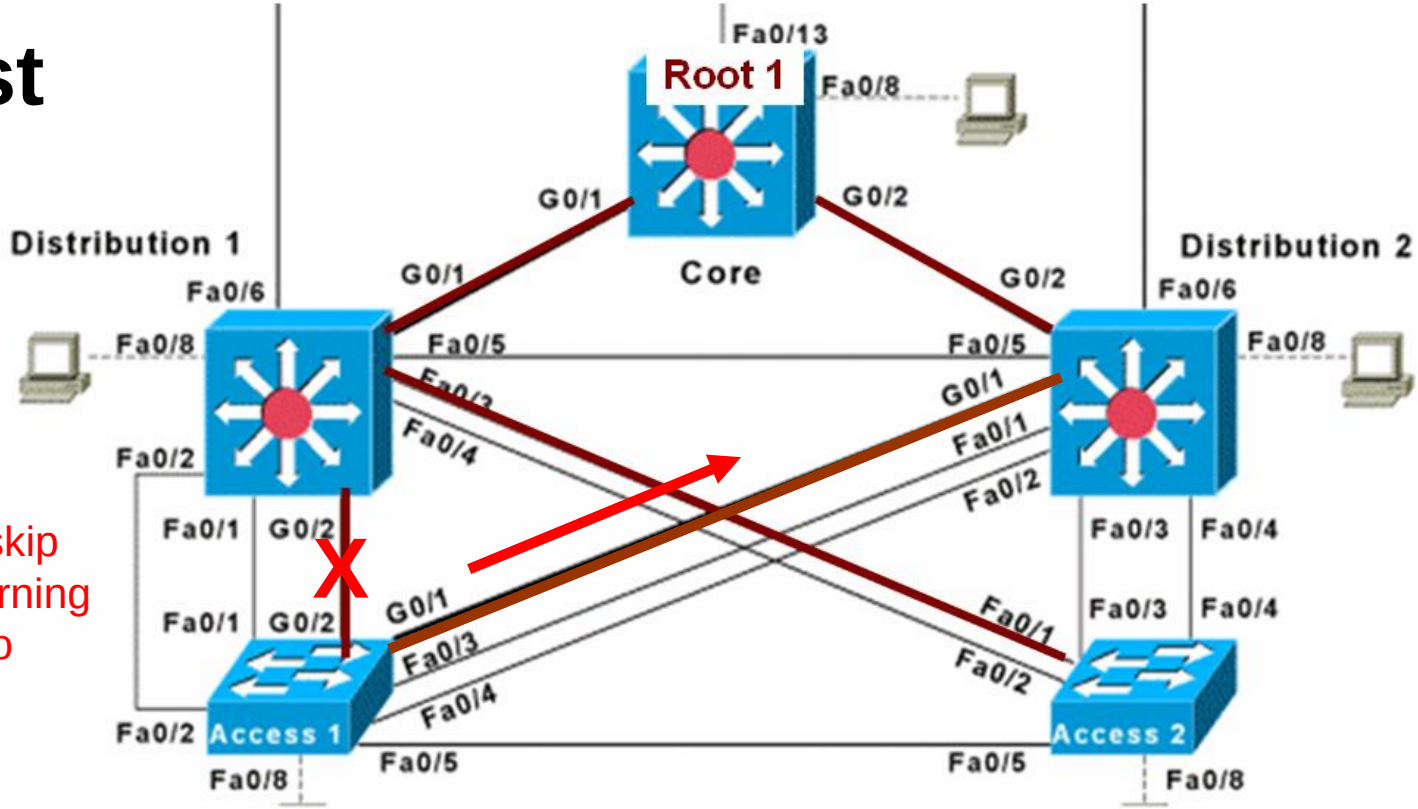
UplinkFast

UplinkFast



- **Uplinkfast** allows access layer switches the ability to converge quickly when a link has failed.
- Allows a blocked port on a switch to almost immediately begin forwarding frames when it detects the failure of the forwarding link.
- Uplinkfast is designed for to only operate on switches that are “leaves” (end nodes) of the spanning tree.
- Uplinkfast is **not** designed for use within backbone or distribution switches.

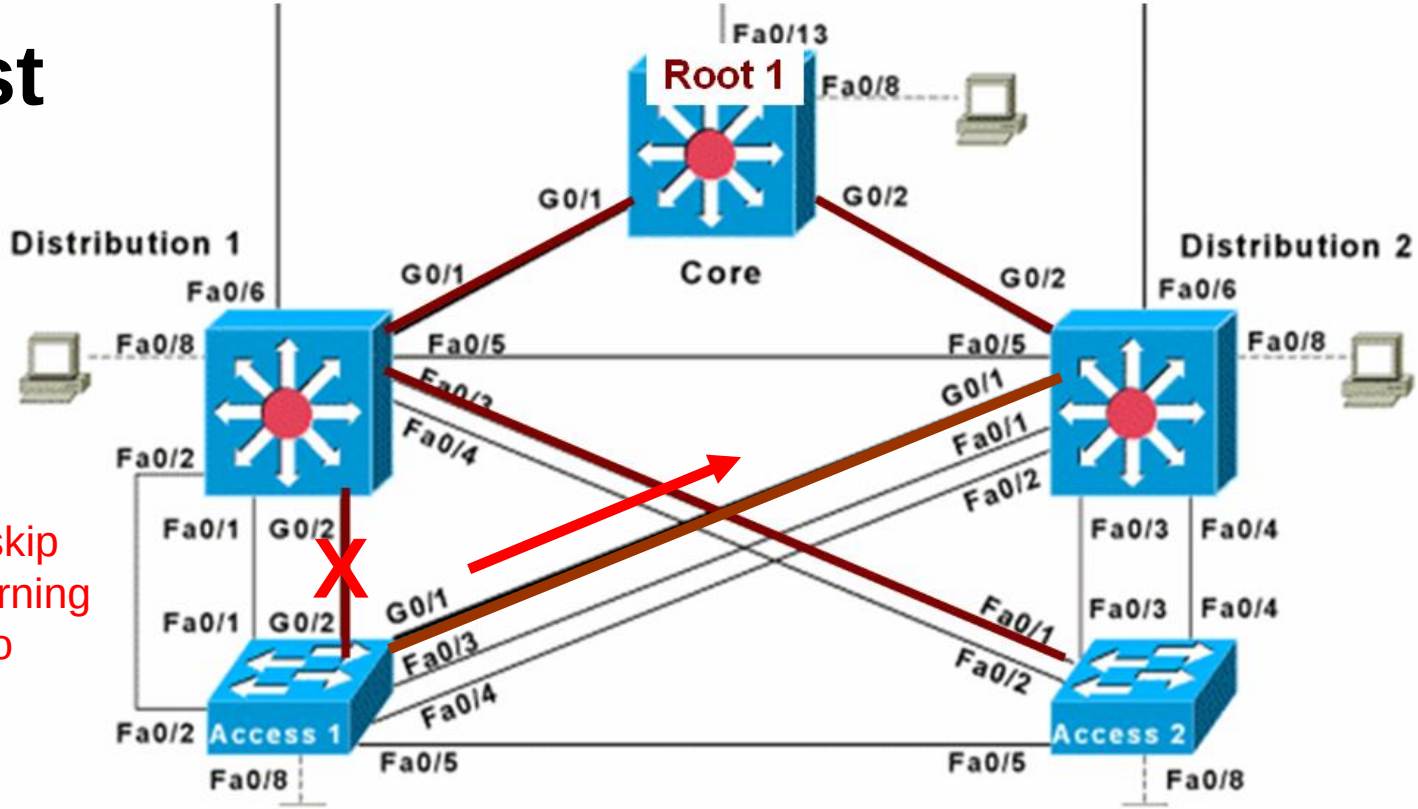
UplinkFast



Unblock G 0/1, skip listening and learning and go directly to forwarding

- UplinkFast must have direct knowledge of the link failure in order to move a blocked port into a forwarding state.
- When Access 1 detects a link failure on the currently active link, the root port (a direct link failure), UplinkFast unblocks the blocked port on Access 1 and transitions it to the forwarding state without going through the listening and learning states.
- This switchover occurs within 5 seconds.

UplinkFast



Unblock G 0/1, skip listening and learning and go directly to forwarding

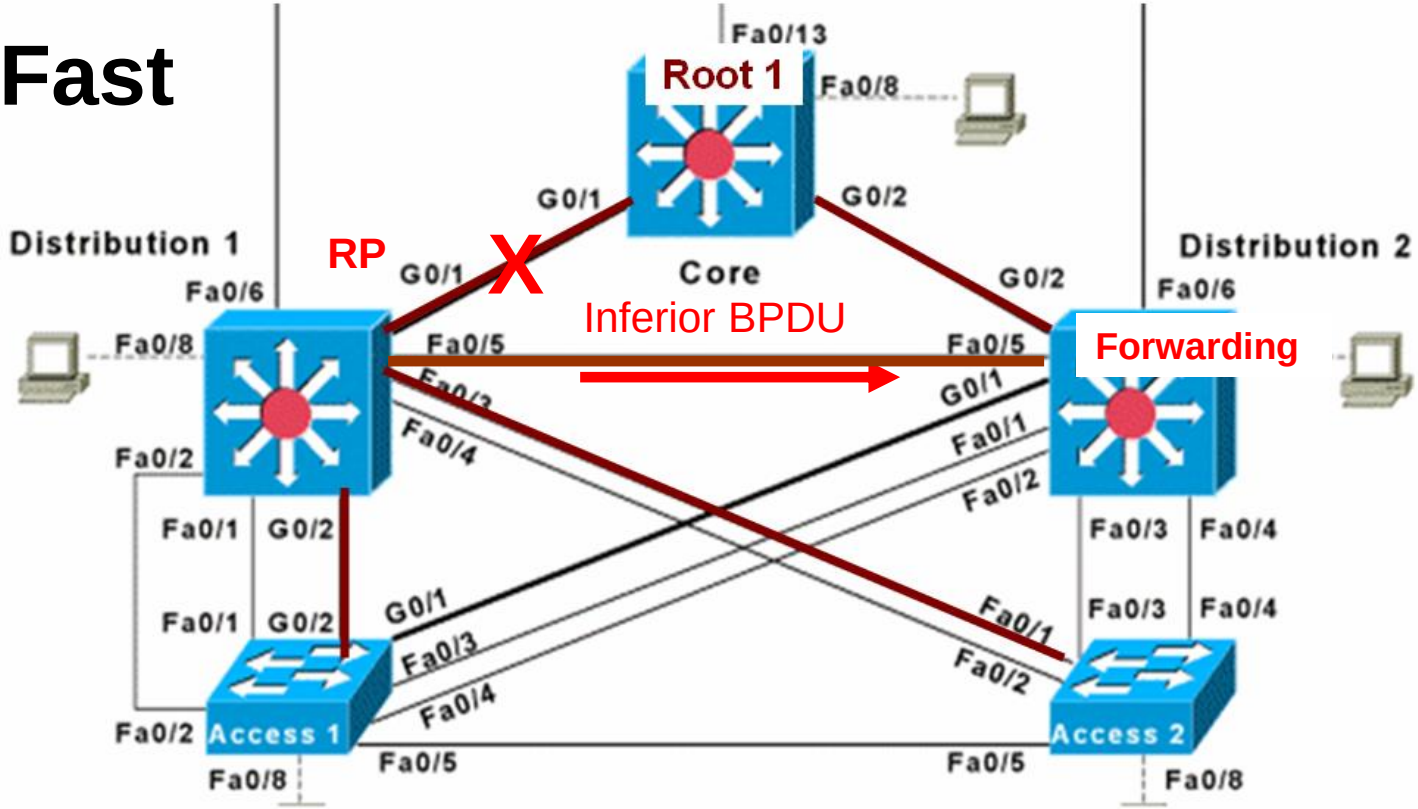
```
Access1(config)#spanning-tree uplinkfast
```

- Cisco switches do not support Uplinkfast on a per-VLAN basis.

BackboneFast

BackboneFast

Backbonefast allows blocked port on Distribution 2 to move immediately to the listening state without waiting for the maximum aging time for the port to expire, and then to forwarding state.



- BackboneFast is initiated when a root port or blocked port on a switch receives **inferior BPDUs** from a designated bridge.
- An inferior BPDU identifies one switch as both the root bridge and the designate bridge.

BackboneFast

Normal BPDU

Bytes	Field
2	Protocol ID
1	Version
1	Message type
1	Flags
8	Root ID = Core
4	Cost of path
8	Bridge ID = Dist1
2	Port ID
2	Message age
2	Max age
2	Hello time
2	Forward delay

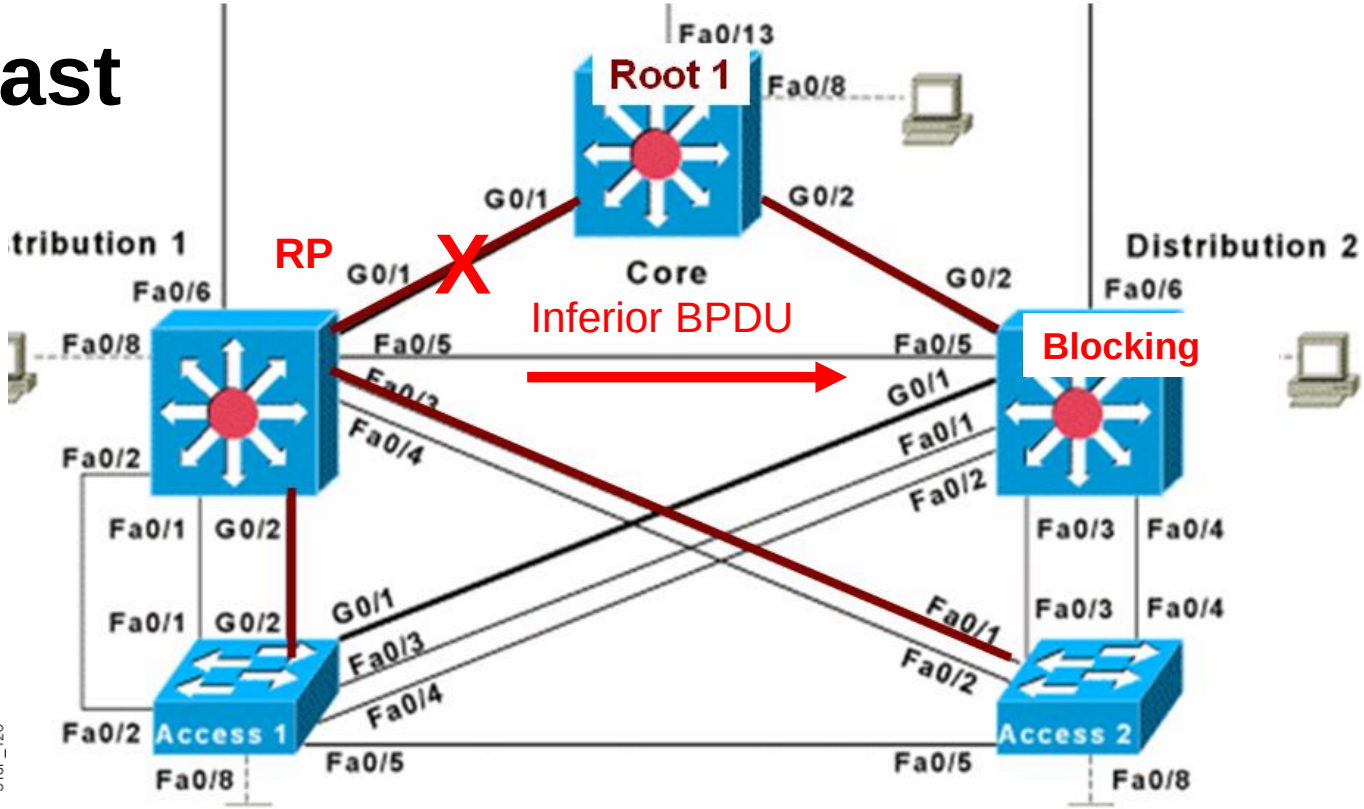
310P_126

Inferior BPDU

2	Protocol ID
1	Version
1	Message type
1	Flags
8	Root ID = Dist1
4	Cost of path
8	Bridge ID = Dist1
2	Port ID
2	Message age
2	Max age
2	Hello time
2	Forward delay

310P_126

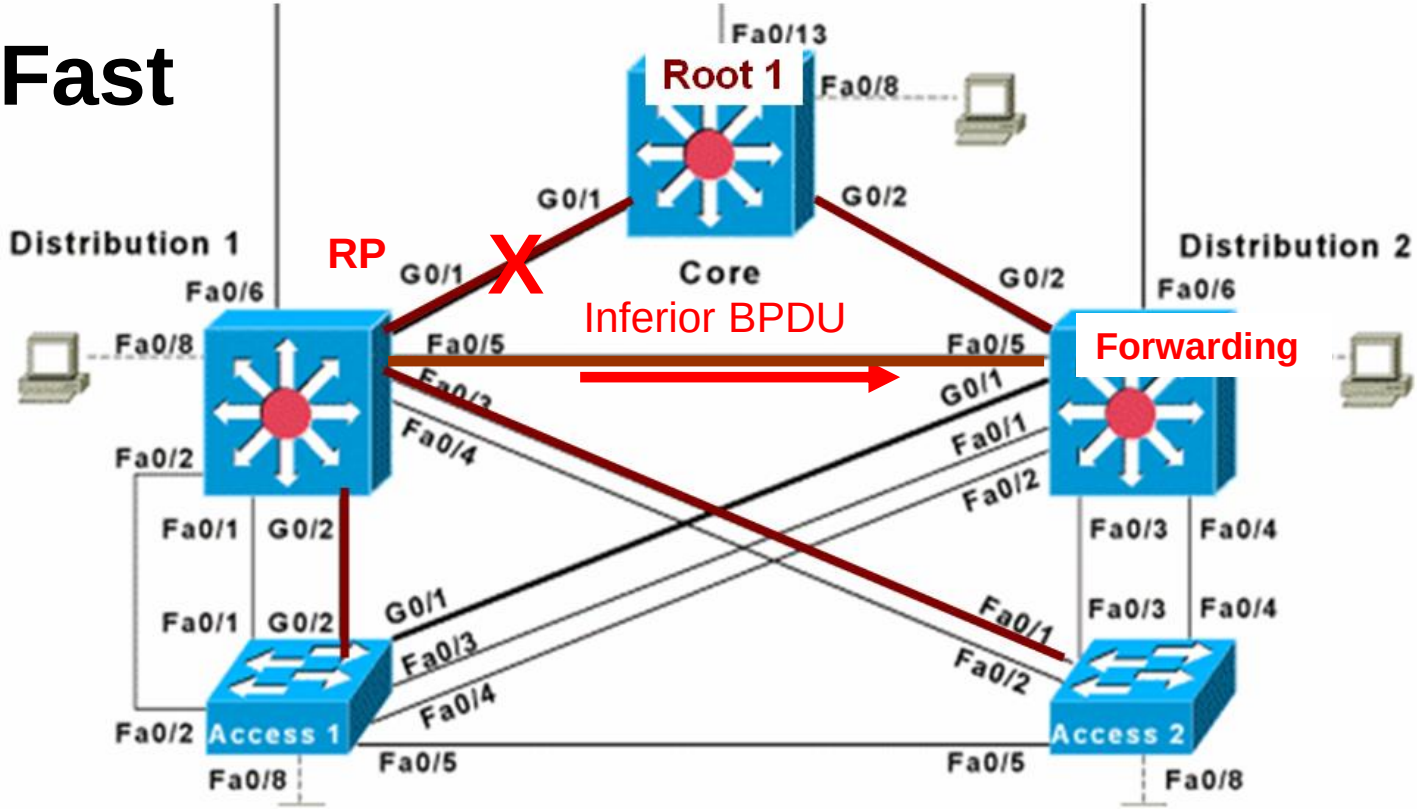
Same Switch



- An **inferior BPDU** identifies one switch as both the root bridge and the designate bridge.
- Distribution 1 is the Designated Bridge.
- *Normally*, sends BPDUs with Root Bridge as the Core BID.
- **Inferior BPDU** – A received BPDU that identifies the root bridge and the designated bridge as the same switch. *("I was only just the Designate Bridge, but now that I can't get to the Root Bridge, so now I am also the Root Bridge.")*

BackboneFast

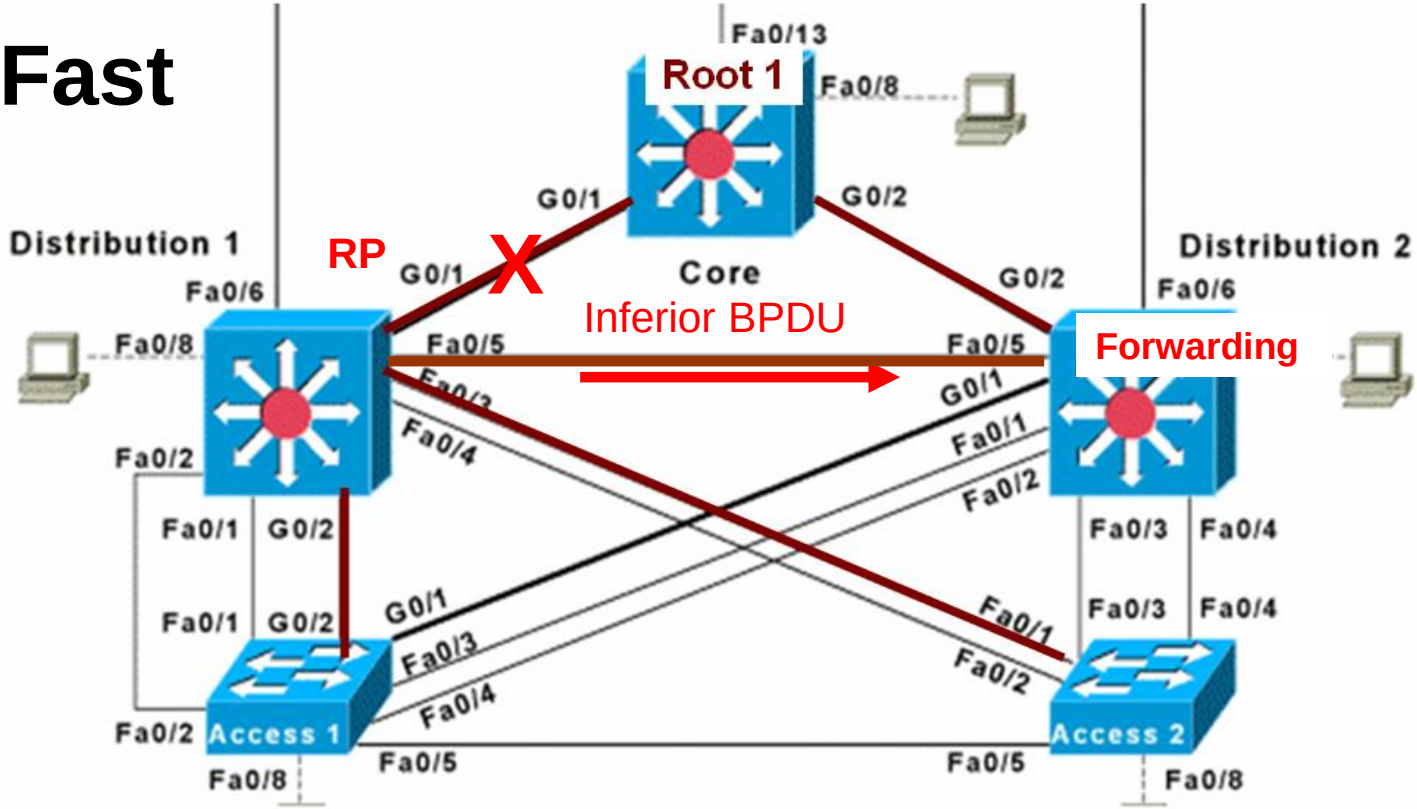
Backbonefast allows blocked port on Distribution 2 to move immediately to the listening state without waiting for the maximum aging time for the port to expire, and then to forwarding state.



- This indicates that a link to which the switch is not directly connected, an indirect link, has failed and the designated switch has lost its connection with the root bridge.
- When a switch receives an inferior BPDU, it indicates that a link to which the switch is not directly connected (an indirect link) has failed (that is, the designated bridge has lost is connection to the root bridge).
- Under normal STP rules, the switch ignores inferior BPDUs for the configured maximum aging time.

BackboneFast

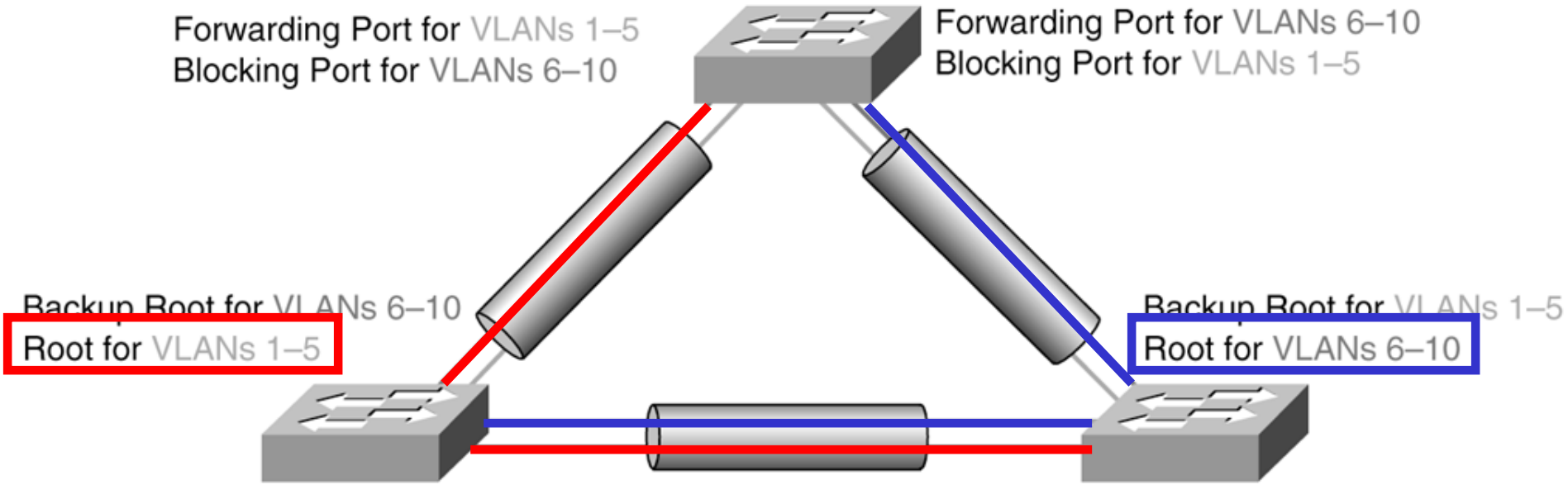
Backbonefast allows blocked port on Distribution 2 to move immediately to the listening state without waiting for the maximum aging time for the port to expire, and then to forwarding state.



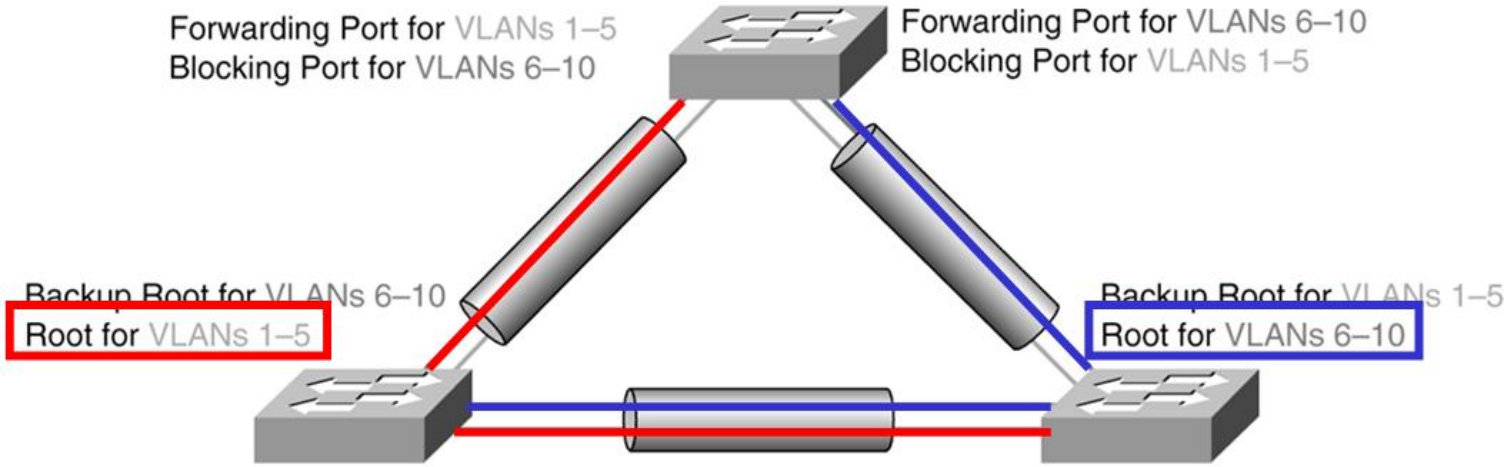
- Link fails, Distribution 2 detects this failure as an indirect failure, since it is not connected directly to that link.
- Distribution 1 no longer has a path to the root switch.
- BackboneFast allows the blocked port on Distribution 2 to move immediately to the listening state without waiting for the maximum aging time for the port to expire.
- BackboneFast then transitions the port on Distribution 2 to the forwarding state, providing a path from Distribution 1 to Distribution 2.
- This switchover takes approximately 30 seconds.

PVST+

PVST+: Per-VLAN Spanning Tree

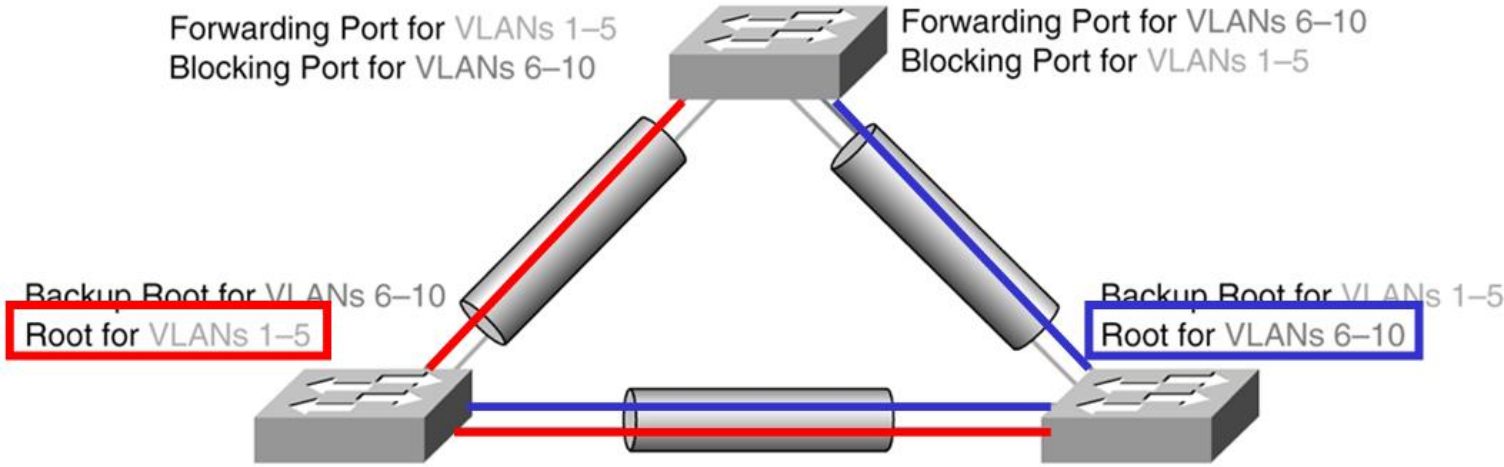


PVST+



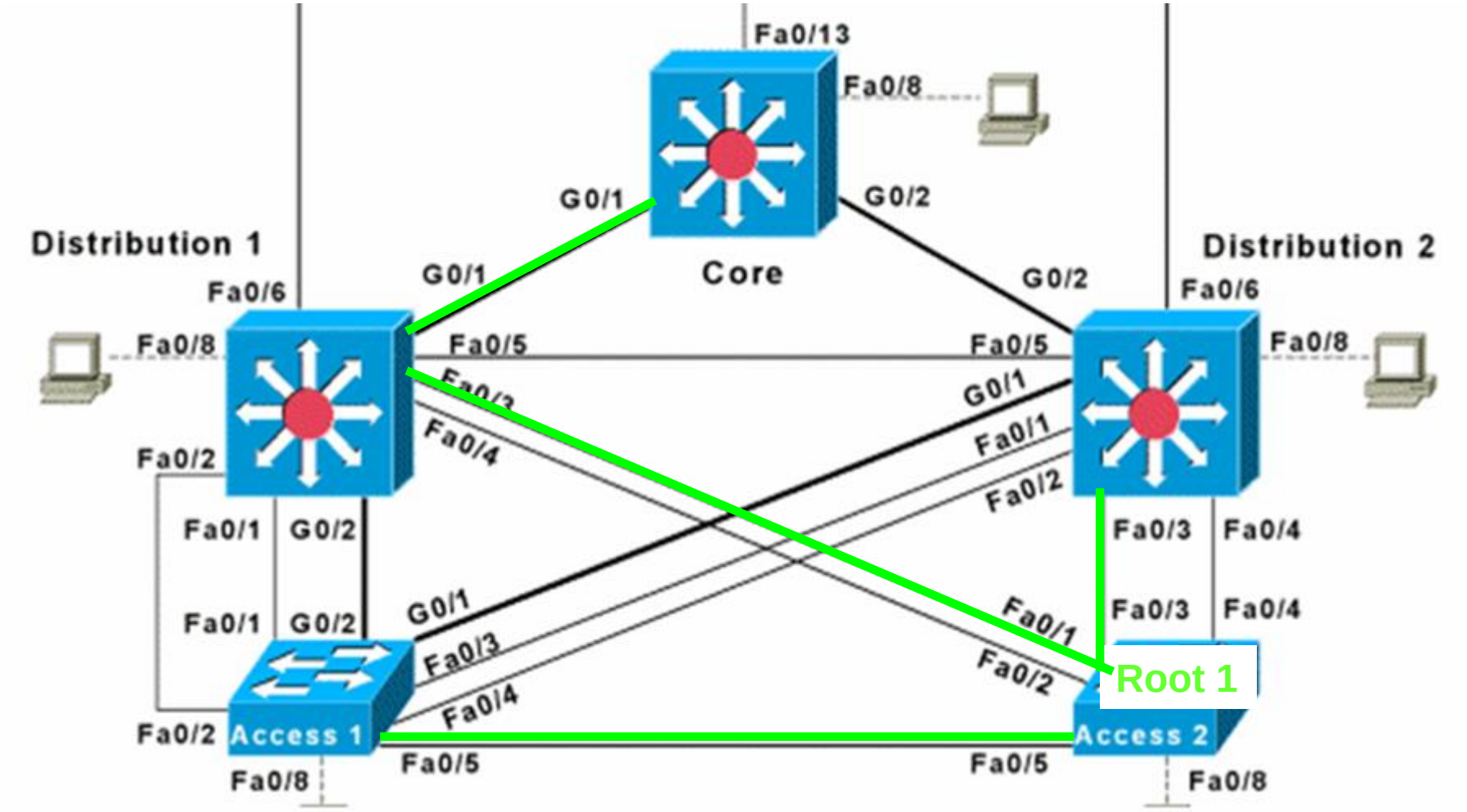
- Per VLAN Spanning Tree Plus (PVST+) maintains a separate spanning-tree instance for each VLAN.
- By default, a single spanning tree runs on each configured VLAN, provided STP has not been manually disabled.
- The plus sign in PVST+ indicates that STP 802.1D has been enhanced by Cisco with proprietary features.
- If configured, PVST+ provides for load balancing on a per-VLAN basis; PVST+ allows creation of different logical topologies using the VLANs on a switched network to ensure that all links can be used and that one link is not oversubscribed.
- Each instance of PVST+ on a VLAN has a single root bridge.

PVST+

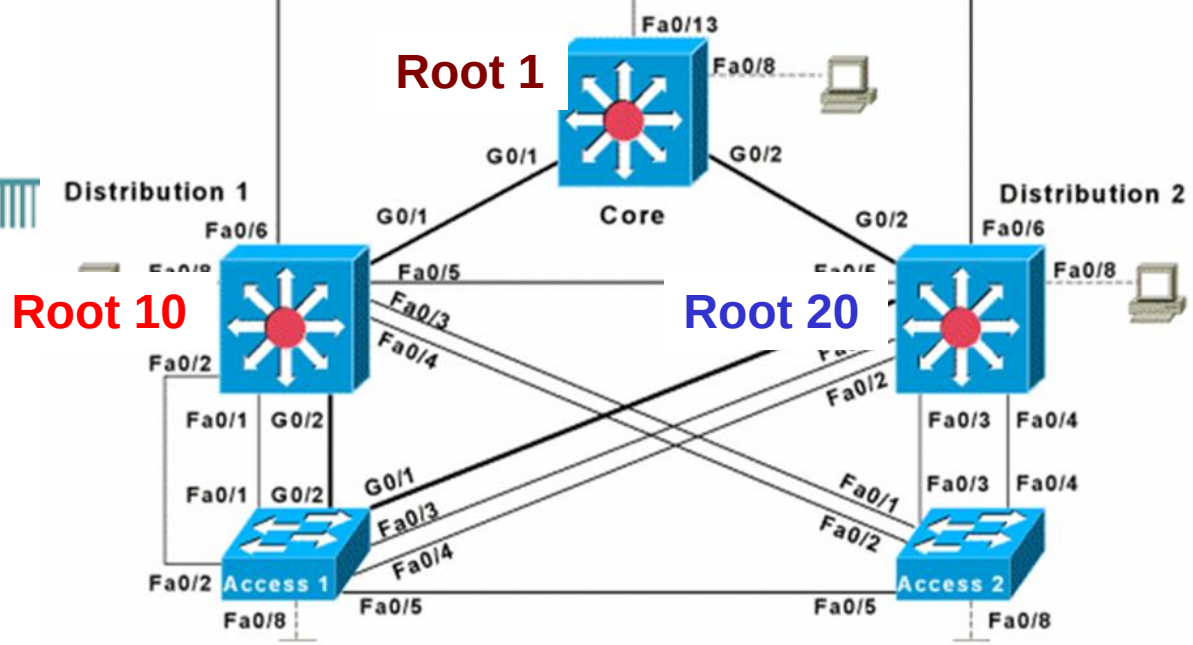


- IEEE 802.1Q VLAN trunks impose limitations on the spanning-tree features in a network.
- In a network of Cisco switches connected through 802.1Q trunks, the switches maintain one instance of spanning tree for each VLAN allowed on the trunks.
- However, non-Cisco 802.1Q switches maintain only one instance of spanning tree for all VLANs allowed on the trunks.

Default: Access2 is the Root for VLAN 1

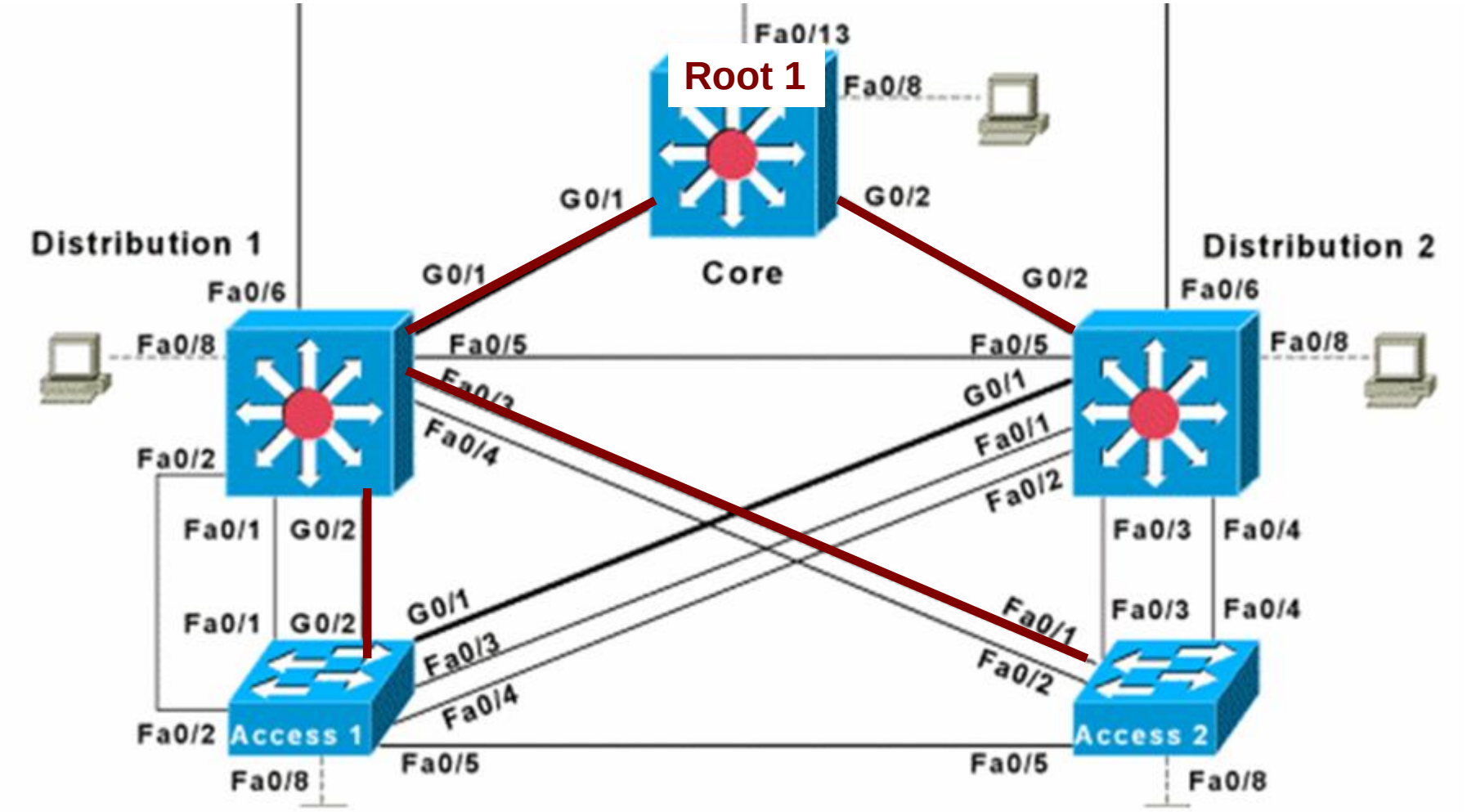


PVST+

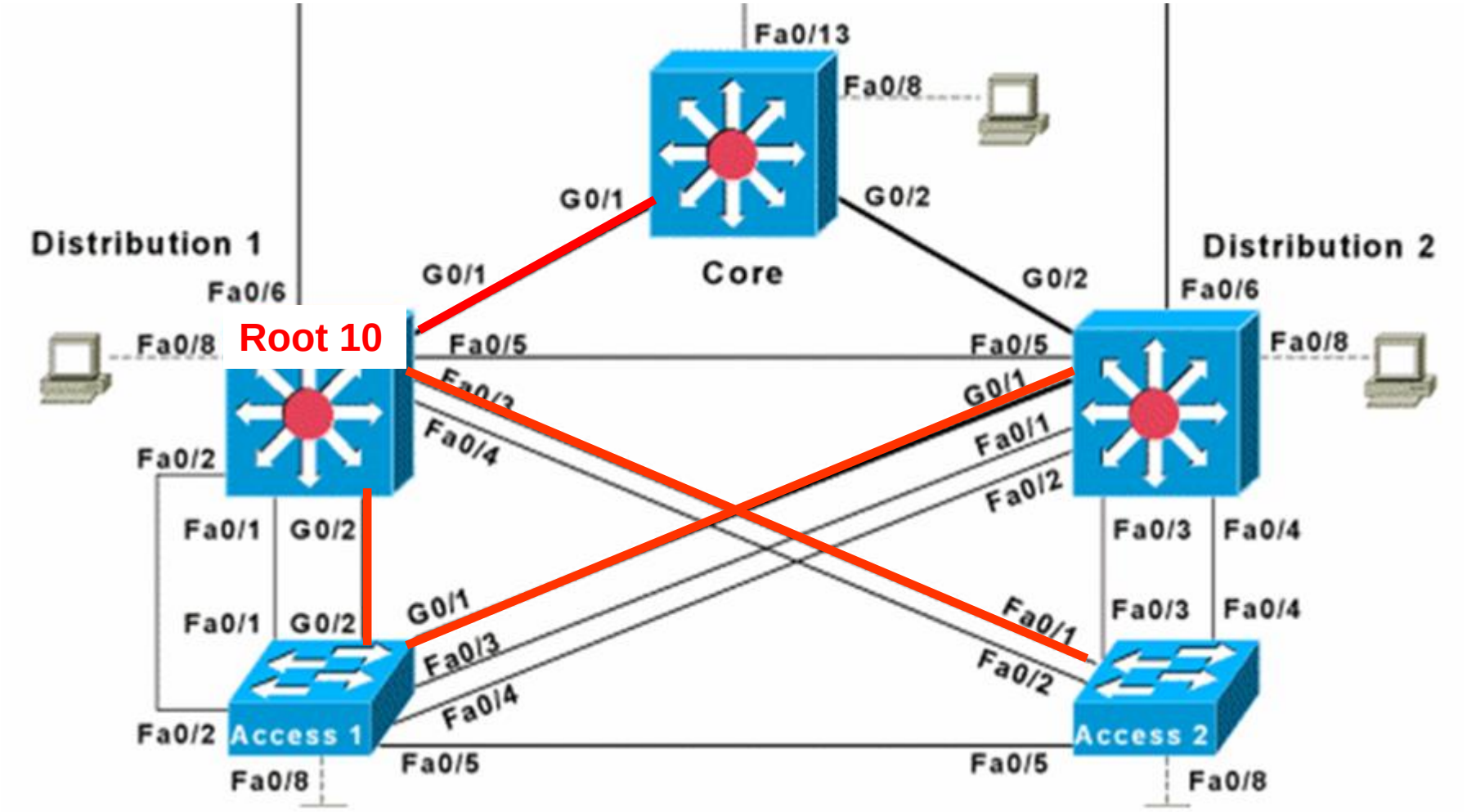



```
Core(config)#spanning-tree vlan 1 root primary

Distribution1(config)#spanning-tree vlan 10 root primary

Distribution2(config)#spanning-tree vlan 20 root primary
```

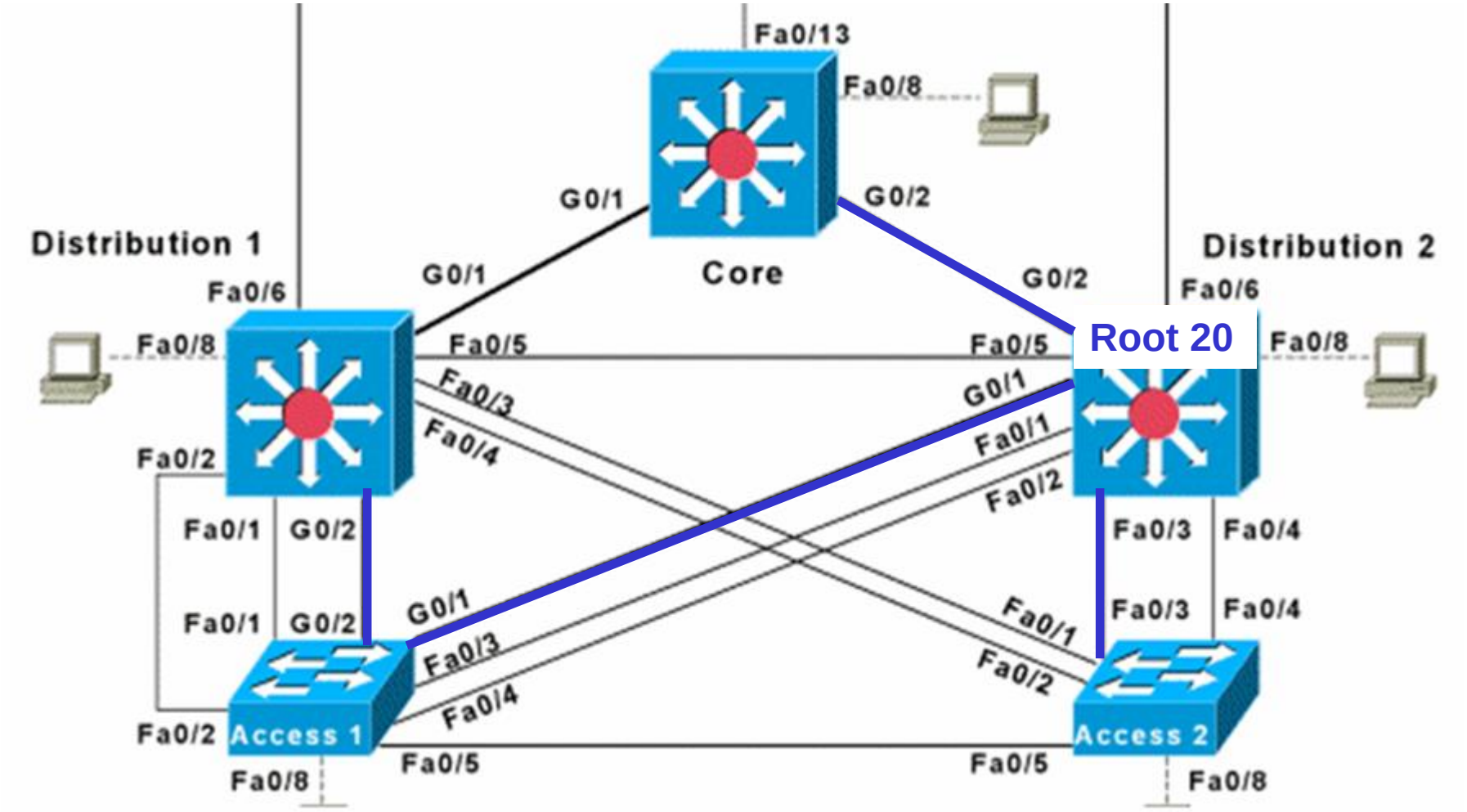
Core is the Root for VLAN 1



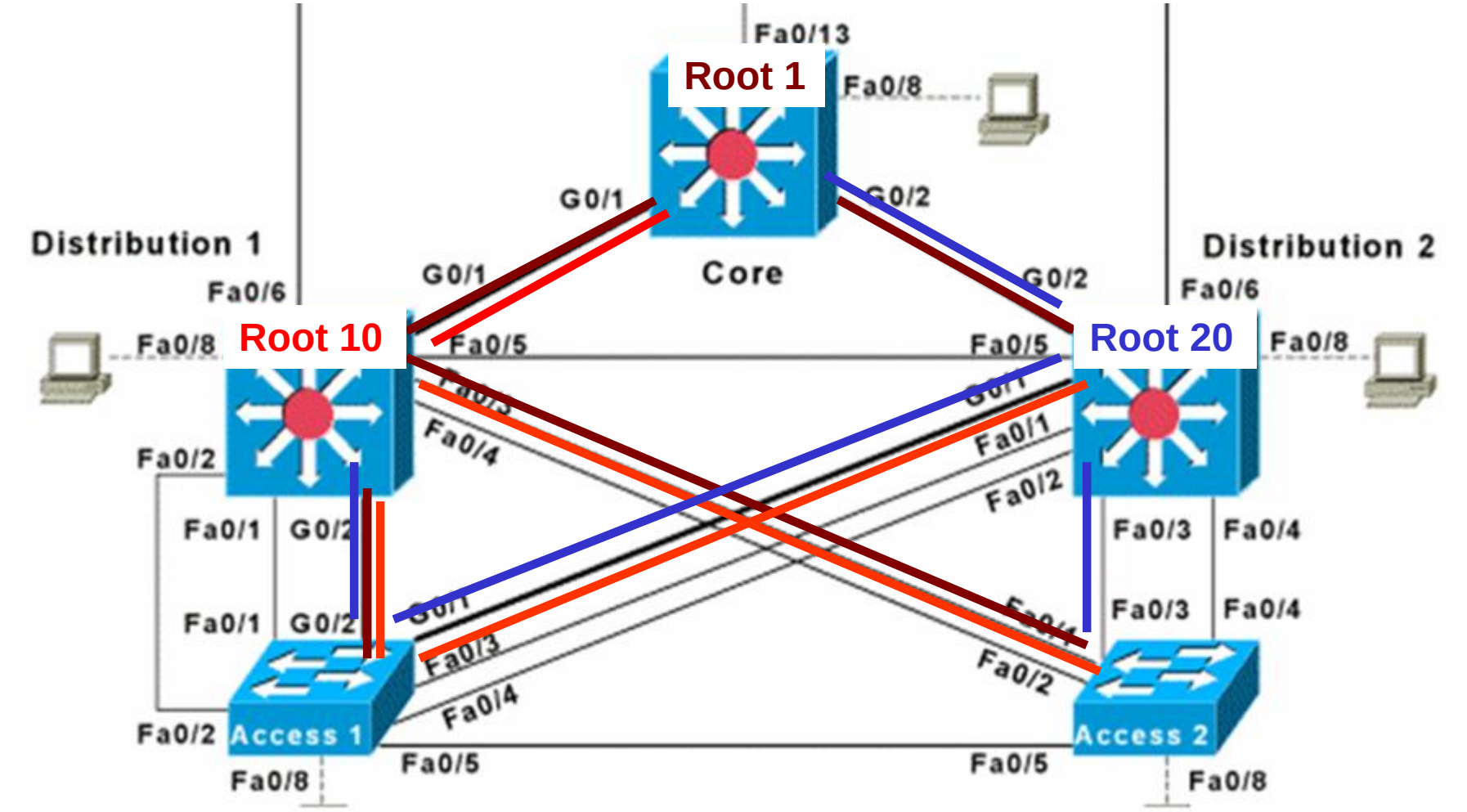
Distribution1 is the Root for VLAN 10



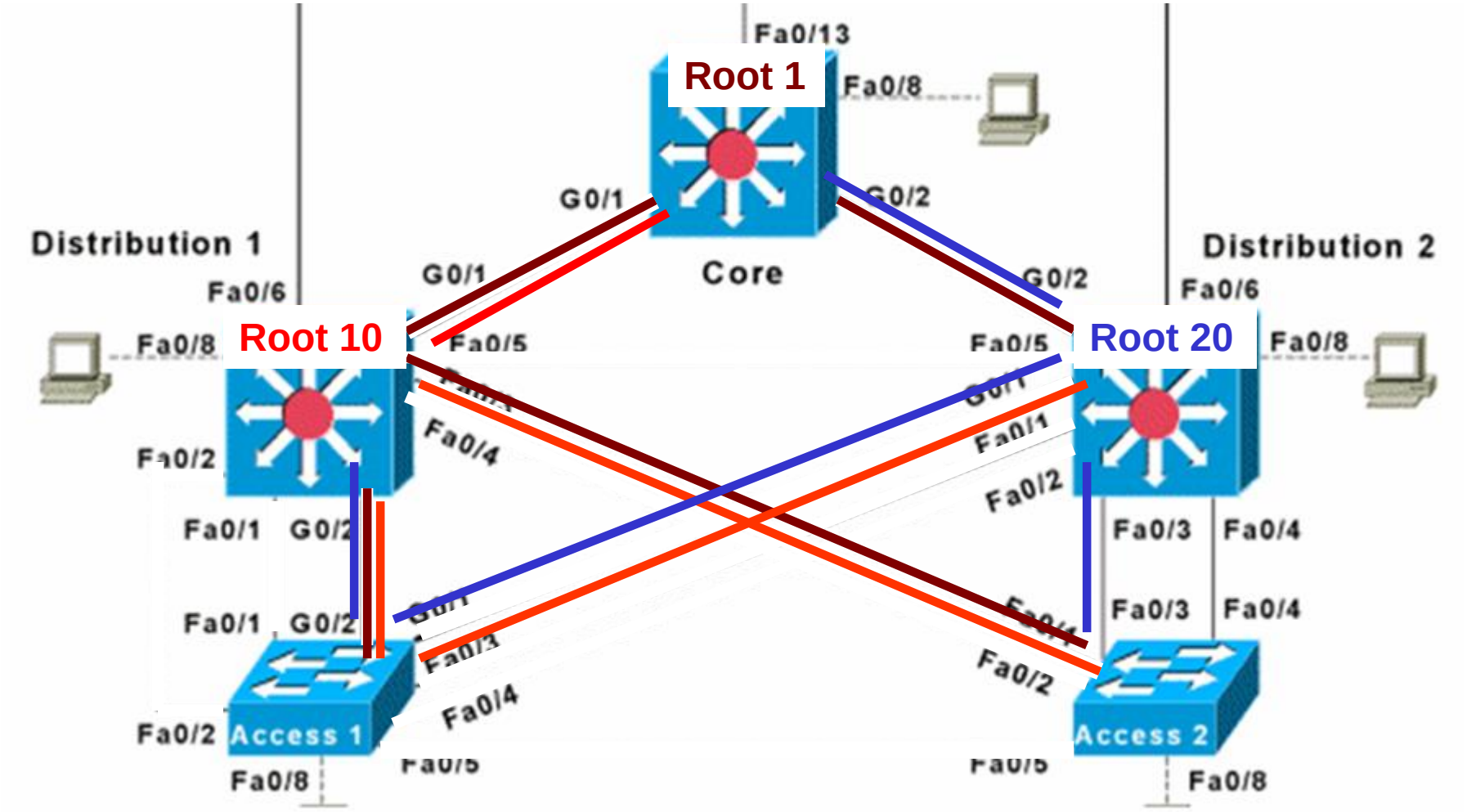
Distribution2 is the Root for VLAN 20



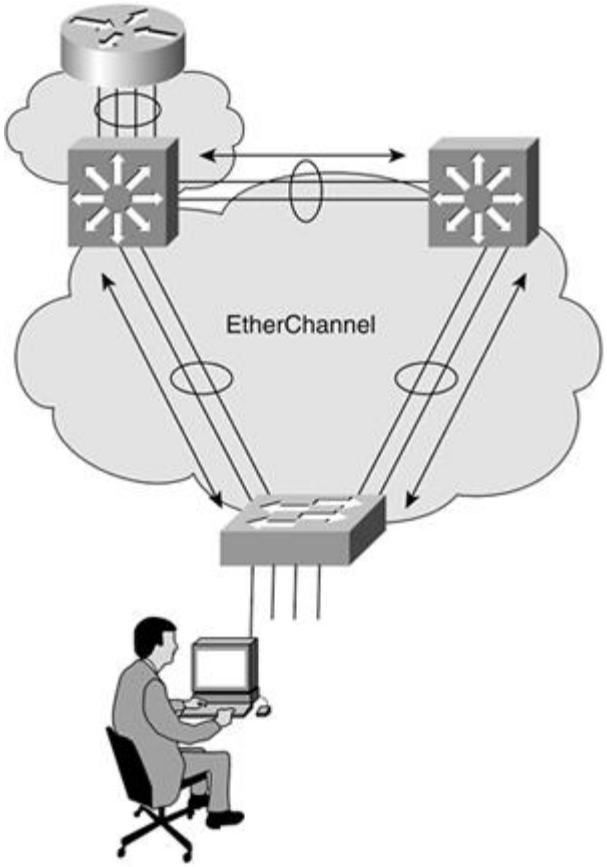
Load Balancing with 3 Root Switches



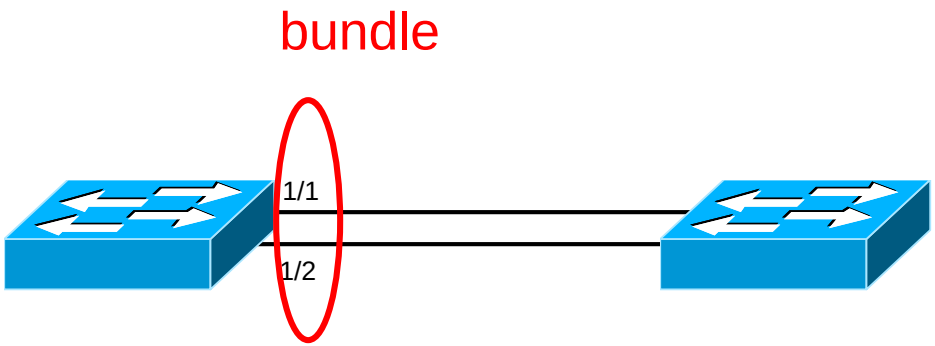
Load Balancing with 3 Root Switches



EtherChannel



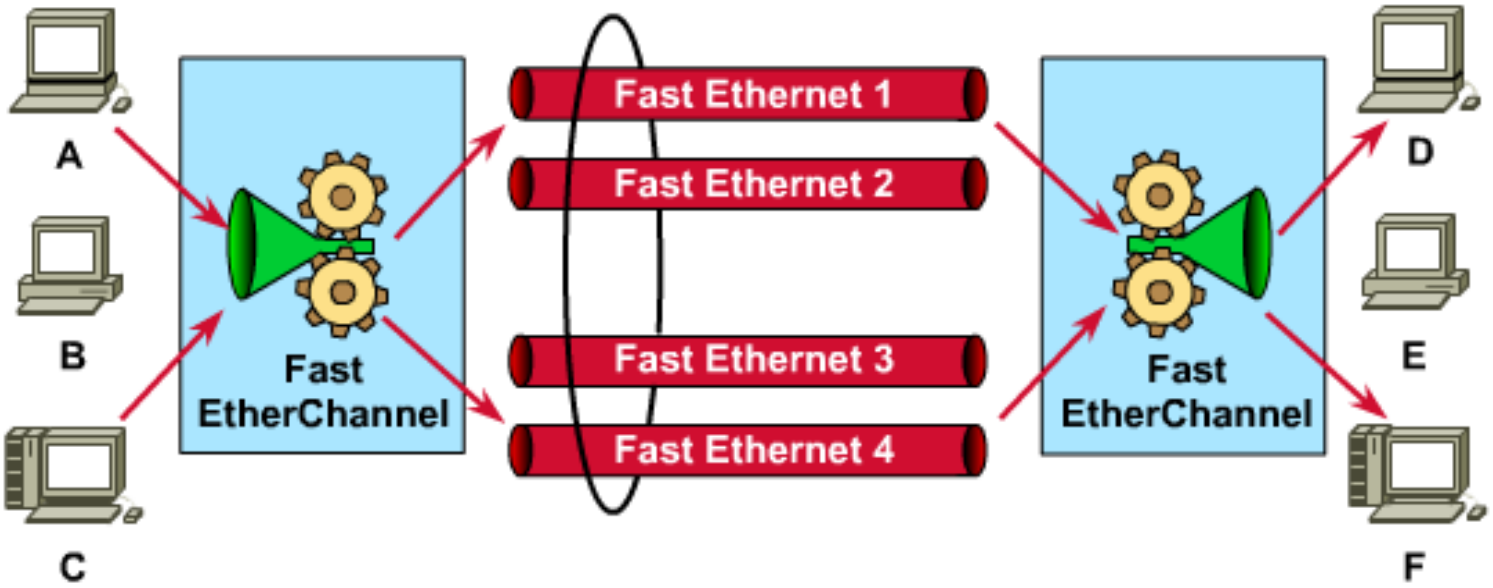
EtherChannel



Can we use both of these links together?

Yes! With Fast EtherChannel (FEC), or Gigabit EtherChannel, frames are distributed among both links, allowing them to work together as a channel.

EtherChannel

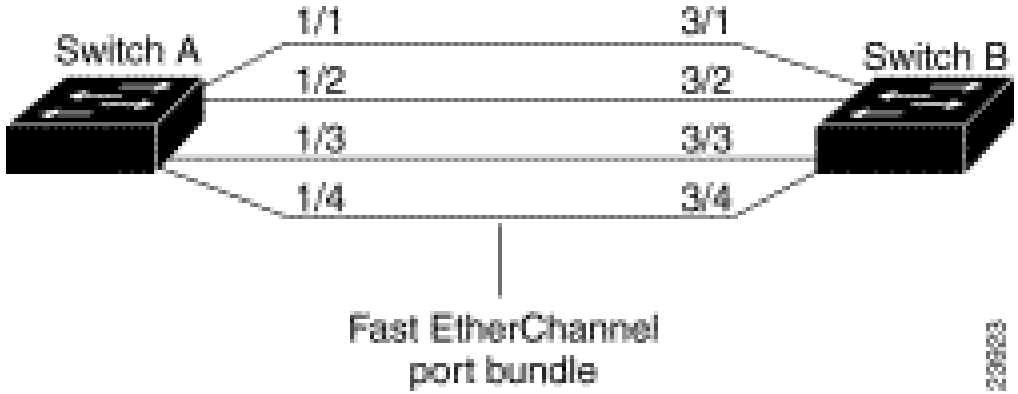


- Allows parallel links to be treated by Spanning Tree as one physical link
- Offers bandwidth scalability within the campus by providing full-duplex bandwidth of 200 to 800 Mbps
- Unicast, multicast, and broadcast traffic is distributed across the links in the channel.
- A bundle is a group of links managed by the EtherChannel process

PAgP and LACP (Management)

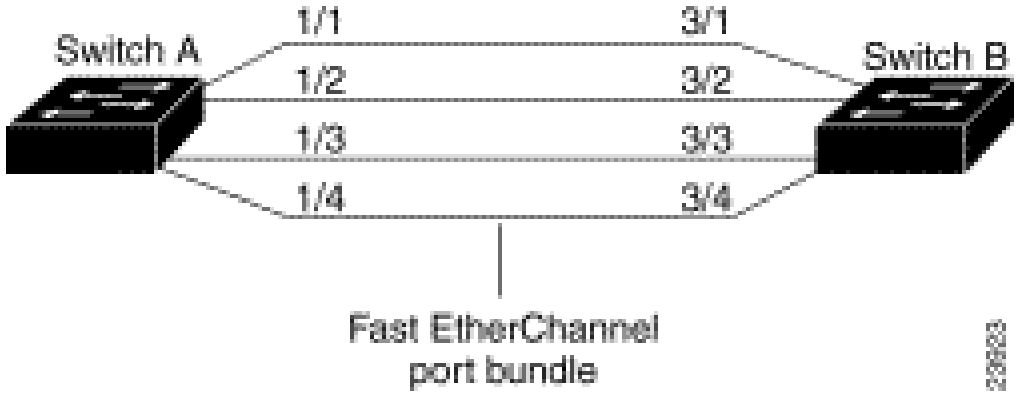
- The Catalyst family of switches supports both:
  - Cisco proprietary Port Aggregation Protocol (PAgP)
  - Industry standard 802.3ad-based protocol Link Aggregation Control Protocol (LACP).
- PAgP is a management function, which checks the parameter consistency at either end of the link and assists the channel in adapting to link failure or addition.
- Both LACP and PAgP prevents STP loops or packet loss due to misconfigured channels and aids network reliability.
- Not many differences.
- When a Cisco switch is connected to a non-Cisco switch use LACP.

Best Practices for EtherChannel



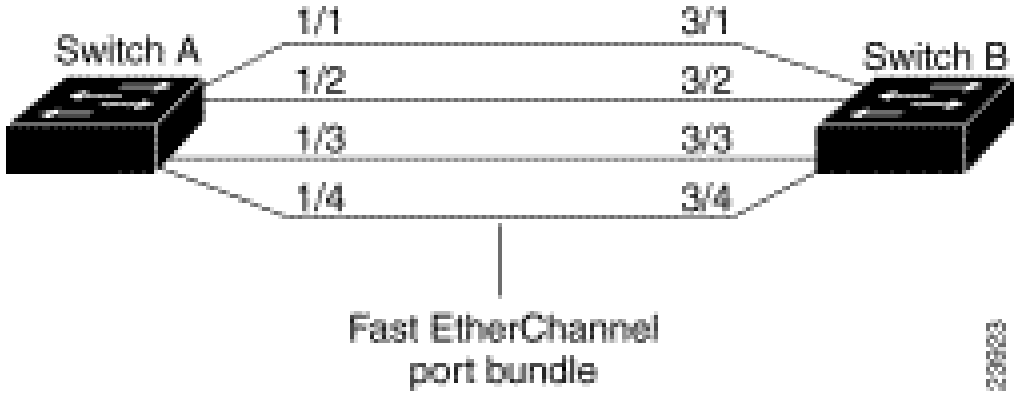
- Cisco switches allow for a maximum of eight ports per EtherChannel. (May be model specific.)
  - The ports do not have to be contiguous or on the same module.
- All ports in an EtherChannel must use the same protocol (PAgP or LACP).
- All ports in an EtherChannel must have the same speed and duplex mode.
  - LACP requires that the ports operate only in full-duplex mode.

Best Practices for EtherChannel



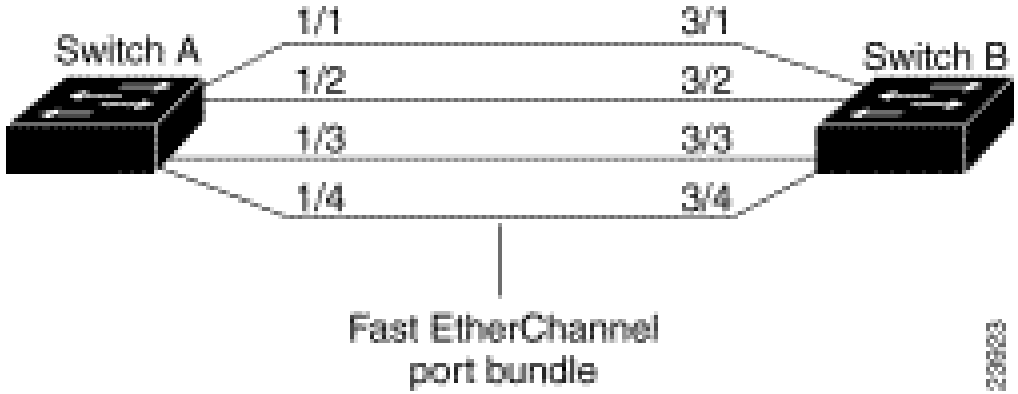
- A port cannot belong to more than one channel group at the same time.
- All ports in an EtherChannel must be configured to be in the same access VLAN configuration or be configured as VLAN trunks with the same allowable VLAN list and the same native VLAN.
- All ports in an EtherChannel require the same trunk mode to avoid unexpected results (for instance, a trunk mode of dot1q desirable).
- All ports in an EtherChannel require the same VLAN cost configuration.

Exam Certification Guide



- **Two to eight links** of either Fast Ethernet (FE) or Gigabit Ethernet (GE) are bundled as one logical link of *Fast EtherChannel (*FEC*)* or *Gigabit EtherChannel (*GEC*)*, respectively.
- This bundle provides a **full-duplex bandwidth (throughput) of up to 1600 Mbps** (8 links of Fast Ethernet) or 16 Gbps (8 links of Gigabit Ethernet).

Exam Certification Guide



- Generally, all bundled ports must first **belong to the same VLAN**.
- If used as a **trunk:**
  - **bundled ports must all be in trunking mode**
  - have the **same native VLAN**
  - pass the **same set of VLANs**
- Each of the ports should also have the **same speed and duplex** settings before they are bundled.
- Bundled ports must also be configured with **identical Spanning Tree settings.**

Exam Certification Guide

- Traffic in an EtherChannel is distributed across the individual bundled links in a deterministic fashion.
- However, the **load is not necessarily balanced equally** across all the links.
- Instead, frames are forwarded on a specific link as a result of a **hashing algorithm**.
- The algorithm can use:
  - source IP address
  - destination IP address
  - combination of source and destination IP addresses
  - source and destination MAC addresses
  - TCP/UDP port numbers.
- If **two addresses or port numbers are hashed**, a switch performs an **exclusive-OR (XOR)** operation on one or more of the addresses or TCP/UDP port numbers as an index into the bundled links.

Exam Certification Guide

- Use the following command to configure frame distribution for all EtherChannel switch links:
- `Switch(config)# port-channel load-balance method`

Table 8-3: Types of EtherChannel Load-Balancing Methods

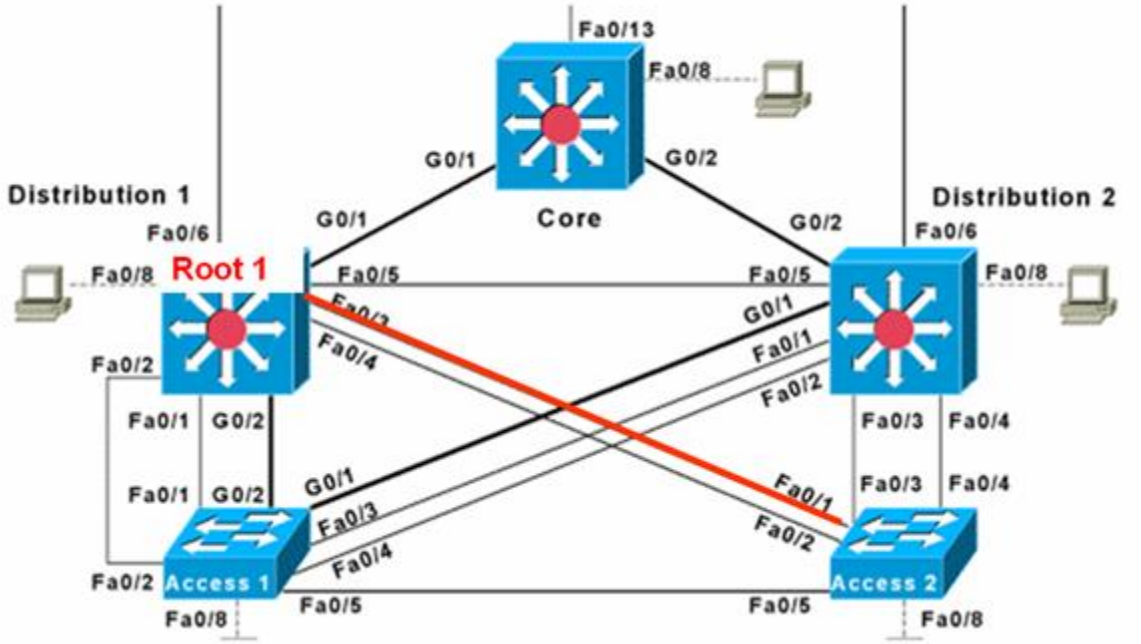
method Value	*Hash input*	*Hash operation*	*Switch Model*
src-ip	Source IP address	bits	6500/4500
dst-ip	Destination IP address	bits	6500/4500
src-dst-ip	Source and destination IP address	XOR	6500/4500/3550
src-mac	Source MAC address	bits	6500/4500/3550
dst-mac	Destination MAC address	bits	6500/4500/3550
src-dst-mac	Source and destination MAC	XOR	6500/4500
src-port	Source port number	bits	6500/4500
dst-port	Destination port number	bits	6500/4500
src-dst-port	Source and destination port	XOR	6500/4500

Exam Certification Guide

Here are some reminders about EtherChannel operation and interaction:

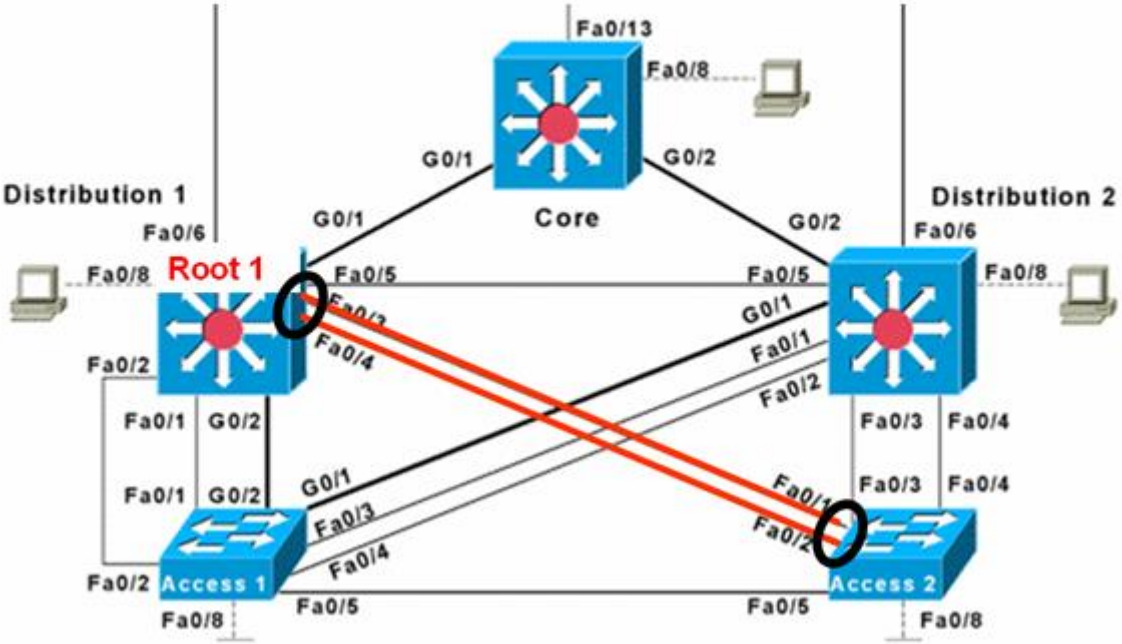
- EtherChannel ***on*** mode does not send or receive PAgP or LACP packets. Therefore, both ends should be set to the ***on*** mode.
- EtherChannel ***desirable*** (PAgP) or ***active*** (LACP) mode attempts to ask the far end to bring up a channel. Therefore, the other end must be set to either ***desirable*** or ***auto*** mode.
- EtherChannel ***auto*** (PAgP) or ***passive*** (LACP) mode participates in the channel protocol, but only if the far end asks for participation. Two switches in the ***auto*** or ***passive*** mode will not form an EtherChannel.
- PAgP ***desirable*** and ***auto*** modes default to the ***silent*** submode, where no PAgP packets are expected from the far end. If ports are set to ***non-silent*** submode, PAgP packets must be received before a channel will form.

Before Fast EtherChannel



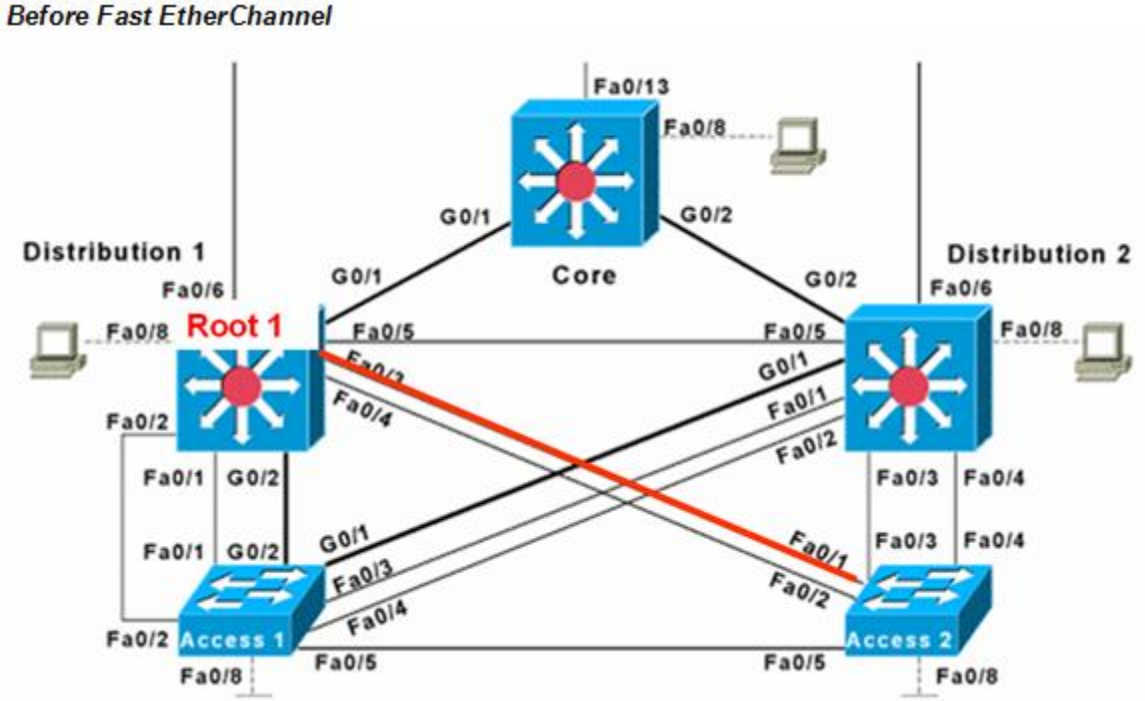
Cabrillo College

After FastEtherChannel



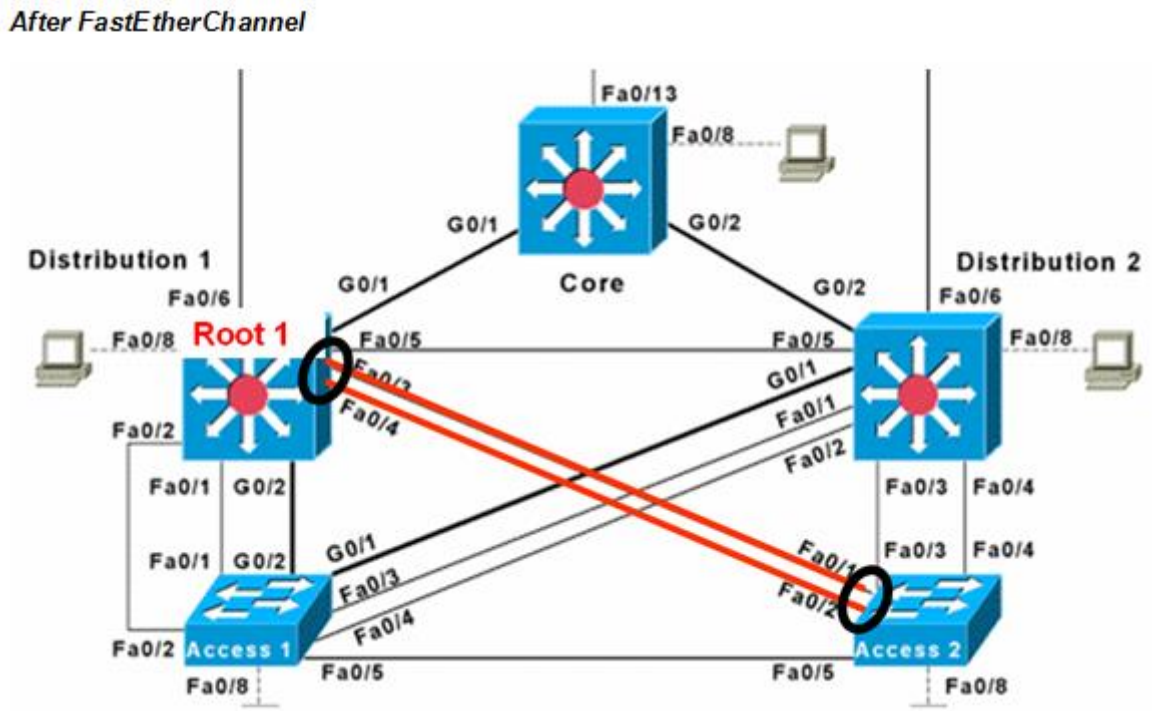
Rick Graziani graziani@cabrillo.edu

Before EtherChannel



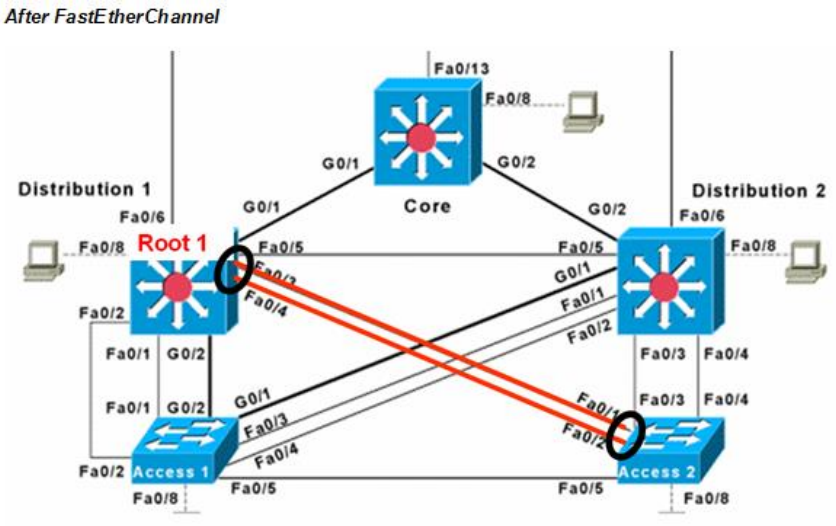

```
Access2#show spanning-tree
<Output omitted>
              Aging Time 300
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------
Fa0/1            Root FWD 19        128.1    P2p
Fa0/2            Altn BLK 19        128.2    P2p
Fa0/3            Altn BLK 19        128.3    P2p
Fa0/4            Altn BLK 19        128.4    P2p
Fa0/5            Altn BLK 19        128.5    P2p
```

EtherChannel




```
Distribution1(config)#interface range fa 0/3 - 4
Distribution(config-if-range)#channel-group 1 mode desirable

Access2(config)#interface range fa 0/1 - 2
Access2(config-if-range)#channel-group 1 mode desirable
```

Verify EtherChannel



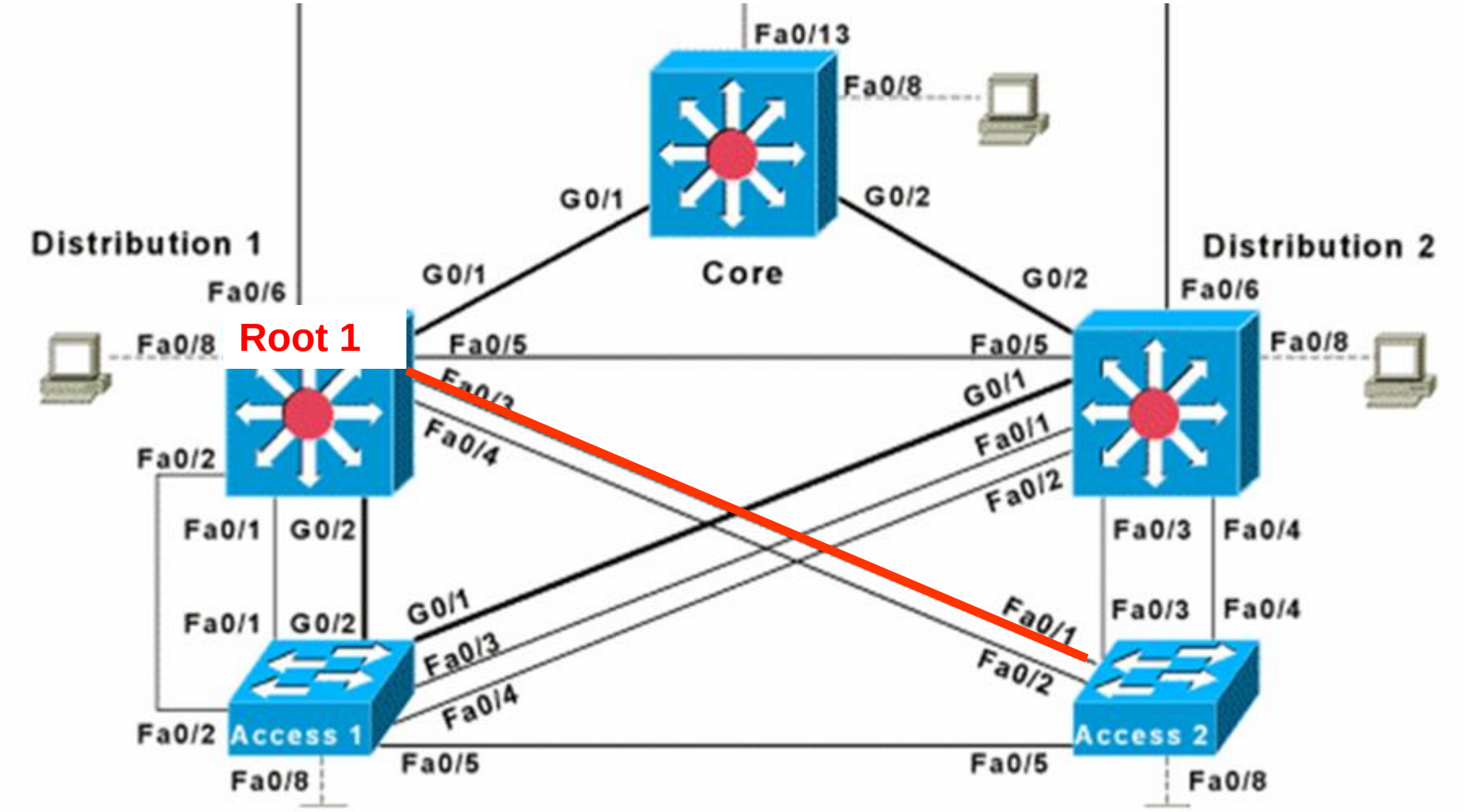

```
Distribution1#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        R - Layer3      S - Layer2
        u - unsuitable for bundling
        U - port-channel in use
        d - default port
Group Port-channel  Ports
------+-------------+-----------------------------------------------
1     Po1(SU)     Fa0/3(P)   Fa0/4(P)
```

```
Access2#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        u - unsuitable for bundling
        U - in use      f - failed to allocate aggregator
        d - default port
Number of channel-groups in use: 1
Number of aggregators:           1
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)         PAgP      Fa0/1(Pd)   Fa0/2(P)
```

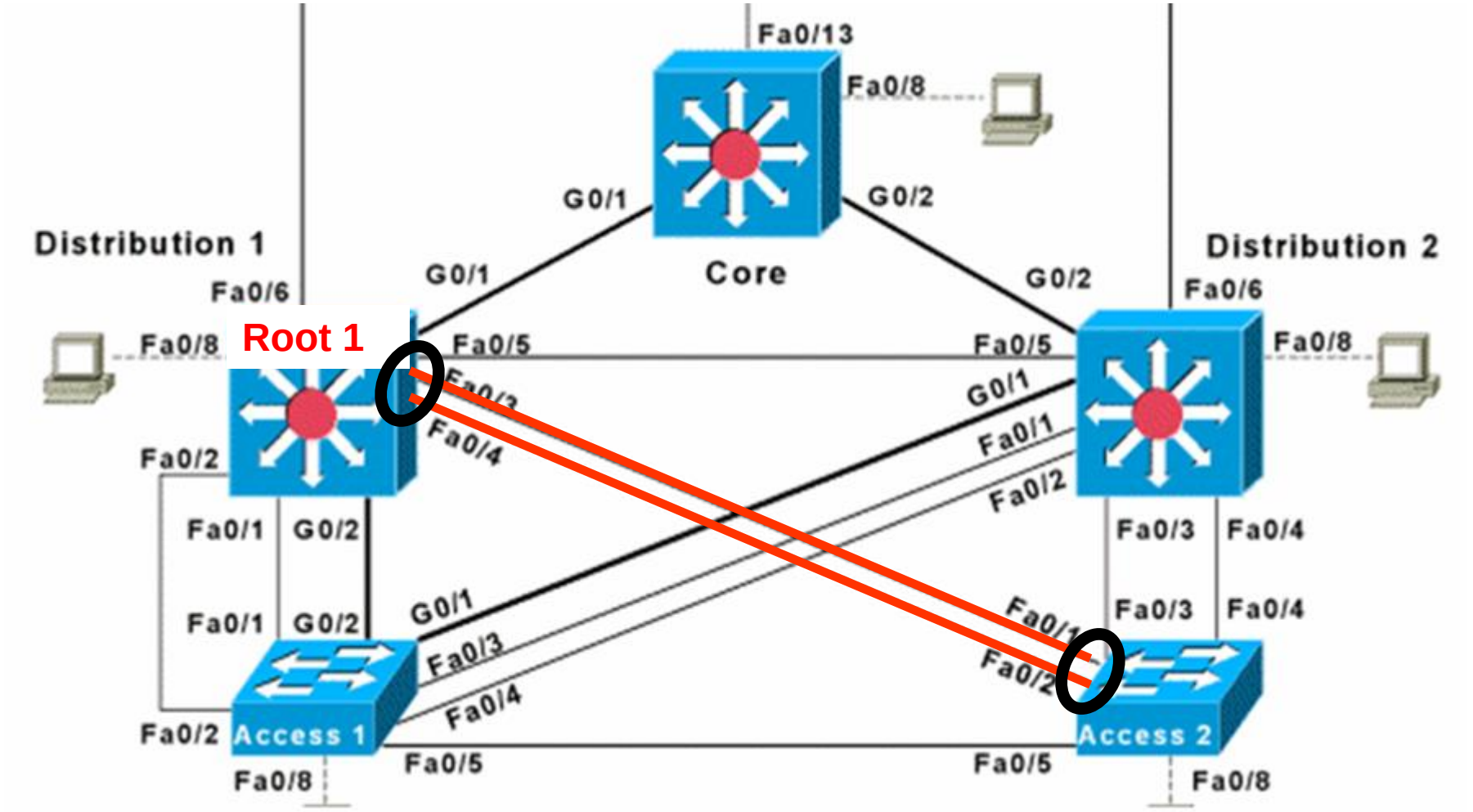
Verify EtherChannel


```
Distribution1#show spanning-tree
<Output omitted>
Interface        Port ID                         Designated                 Port ID
Name             Prio.Nbr      Cost Sts      Cost Bridge ID
   Prio.Nbr
---------------- -------- --------- --- --------- -------------------- -------
Fa0/1            128.1            19 FWD          0 24577 000b.fd13.9080 128.1
Fa0/2            128.2            19 FWD          0 24577 000b.fd13.9080 128.2
Fa0/5            128.5            19 FWD          0 24577 000b.fd13.9080 128.5
Gi0/1            128.25            4 FWD          0 24577 000b.fd13.9080 128.25
Gi0/2            128.26            4 FWD          0 24577 000b.fd13.9080 128.26
Po1              128.65           12 FWD          0 24577 000b.fd13.9080 128.65

Access2#show spanning-tree
VLAN0001
  <Output omitted>
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/3            Altn BLK 19        128.3    P2p
Fa0/4            Altn BLK 19        128.4    P2p
Fa0/5            Altn BLK 19        128.5    P2p
Po1              Root FWD 12        128.65   P2p
```

Distribution1 is the Root for VLAN 1



Distribution1 is the Root for VLAN 1 with Fast EtherChannel



Enhancements to 802.1D and PVST+

Cabrillo College

CIS 187 Multilayer Switched Networks

CCNP 3 version 4

Rick Graziani

Fall 2006